Р. БЭР

ЛИНЕЙНАЯ АЛГЕБРА И ПРОЕКТИВНАЯ ГЕОМЕТРИЯ

Перевод с английского
Е. Г. ШУЛЬГЕЙФЕРА

Предисловие
А. Г. КУРОША

И * Л
ИЗДАТЕЛЬСТВО
ИНОСТРАННОЙ ЛИТЕРАТУРЫ
Москва—1955

LINEAR ALGEBRA
AND
PROJECTIVE GEOMETRY

by R. BAER

New York
1952

ПРЕДИСЛОВИЕ К РУССКОМУ ПЕРЕВОДУ

В заглавии книги Р. Бэра стоят соединенные союзом «и» названия двух важных и уже давно сложившихся ветвей математики — линейной алгебры и проективной геометрии. В действительности же эта книга посвящена изложению одной математической дисциплины, новой и еще не получившей названия, но уже успевшей накопить большое содержание и обладающей достаточно четко очерченной областью исследования. Этот новый раздел математики целиком относится к алгебре, и вместе с тем он поглощает по существу все основное содержаиие проективной геометрии. Благодаря выходу рассматриваемой книги широкие круги математиков получают возможность ознакомиться с сегодияшним состоянием проективной геометрии и, быть может, впервые узнать, что проективная геометрия должна сейчас рассматриваться уже не как ветвь геометрии, а как органическая составная часть алгебры.

Создание проективной геометрии явилось одним из крупных достижений математики девятнадцатого века, оказавшим заметное влияние на развитие всей математики. При этом, говоря о проективной геометрии, мы отделяем ее от алгебраической геометрии — которая, к слову сказать, по существу также целиком относится к области алгебры, являясь всего лишь теорией систем нелинейных алгебраических уравнений,— и от общей теории неэвклидовых геометрий, если относить к последней и вопросы проективного метроопределения. Можно сказать, что развитие проективной геометрии шло в девятнадцатом веке по программе, идущей от Штаудта, т. е., говоря современным языком, в направлении изучения линейных подпространств векторного пространства, их проекций, пересечений и объединений. Понятия и методы, связанные с непрерывностью, играли, конечно, в этом развитии некоторую роль, но не они определяли истиное лицо проективной геометрии. Вместе с тем уровень, достигнутый к тому времени алгеброй, еще не давал

возможности усмотреть в проективной геометрии алгебраической науки.

На рубеже девятнадцатого и двадцатого веков крупный вклад в проективную геометрию сделал Гильберт, показав, что все конечномерные дезарговы проективные геометрии исчерпываются системами линейных подпространств конечномерных векторных пространств над ассоциативными (хотя не обязательно коммутативными) телами. Это был большой шаг в направлении включения проективной геометрии в алгебру, что стало ясным, впрочем, лишь позже, в начале тридцатых годов, когда общая теория ассоциативных колец и тел уже получила некоторое развитие. Приведу, например, следующее весьма образное высказывание П. С. Александрова из его предисловия к русскому переводу книги М. Бохера «Введение в высшую алгебру» (М.—Л., 1933):

«Одной из основных особенностей развития математики в последнее время является проникновение алгебраических понятий, методов и идей в самые различные области математической науки. Один из первых примеров такой а л г е б р а и з а ц и и математических дисциплин дает нам проективная геометрия; несколько сгущая краски, можно сказать, что геометрия проективных аксиом соединения и алгебра наиболее общих алгебраических тел имеют один и тот же реальный субстрат своих построений».

Нужно сказать, что на самом деле в этих словах не было допущено никакого сгущения красок, как показали прошедшие с тех пор два десятилетия. Эти десятилетия были заполнены интенсивной и разносторонней работой алгебраистов по дальнейшему развитию проективной геометрии уже в рамках алгебры. Укажу, например, на полученное Биркгофом описание конечномерных проективных геометрий как дедекиндовых структур, удовлетворяющих некоторым вполне разумным ограничениям; это описание явилось весьма естественным логическим завершением программы Штаудта в ее синтетическом аспекте. Много было сделано и по изучению векторных пространств над ассоциативными телами и систем их линейных подпространств, а также по изучению преобразований этих систем подпространств типа коллинеаций и корреляций. При этом — в полном соответствии с положением в других разделах современной алгебраической науки — был сделан переход к бесконечномерным векториым пространствам, причем, как оказалось, лишь теория

корреляций (т. е. дуальных отображений) не выдерживает этого перехода.

Эти исследования связали проективную геометрию не только с теорией структур и теорией тел, но и со многими другими разделами алгебры. Так, можно отметить связи с общей теорией ассоциативных колец, в частности с теорией простых колец. Очень важны связи с теорией операторных абелевых групп (т. е. модулей над ассоциативными кольцами) и их систем допустимых подгрупп и колец операторных эндоморфизмов. Укажем также на связи с теорией классических групп.

В результате проективная геометрия и многие вопросы алгебры объединились в одну новую алгебраическую науку, которая уже заслуживает того, чтобы получить собственное название. Замечу, что Бэр относит название «линейная алгебра» к общей теории (бесконечномерных) векторных пространств над произвольными (т. е. не обязательно коммутативными, хотя, конечно, ассоциативными) телами. Мне кажется, однако, более целесообразным сохранить это название за тем уже сложившимся и в научном отношении законченным университетским курсом, который посвящен изучению конечномерных векторных пространств над коммутативными полями и их линейных преобразований в связи с теорией матриц. Что же касается нашей новой ветви алгебры, то, быть может, следует называть ее п р о е к т и в н о й а л г е б р о й, если не будет предложено другого названия, более удачного.

Книга Бэра является первой попыткой систематического изложения этой проективной алгебры, притом попыткой безусловно удачной. Сам автор принадлежит к числу виднейших алгебраистов нашего времени; его работы относятся преимущественно к различным вопросам теории групп, но и в область, которой посвящена книга, он сделал существенные вклады. В книге собран и творчески обработан богатый материал. Автору удалось, вместе с тем, придать книге большое внутреннее единство. Он отбрасывает все, что могло бы нарушить это единство, и, например, во избежание осложняющих особенностей, всюду, где это ему полезно, предполагает, что характеристика основного тела отлична от двух или что ранг векторного пространства не меньше трех.

Конечно, вследствие этого стремления автора к единообразию книга Бэра не может дать полного представления о сегодняшнем

состоянии проективной алгебры. Вне книги остается, например, теория недезарговых проективных плоскостей, которая, при всем своеобразии ее предмета и методов, принадлежит, понятно, к рассматриваемой ветви алгебры; читатель найдет, впрочем, хороший обзор этой теории в статье Л. А. Скорнякова «Проективные плоскости», Успехи математических наук 6,6 (1951), 112—154. Не нашла места в книге и интересная, хотя и не получившая пока заметного дальнейшего развития теория непрерывномерных проективных геометрий Дж. Неймана. Далее, автор не излагает и лишь скупо отмечает многие результаты из теории модулей над ассоциативными кольцами, имеющие непосредственное отношение к содержанию книги, хотя именно сюда относится его основной личный вклад и именно в этом направлении следует ожидать в ближайшие годы дальнейшего развития исследований. Наконец, автор избегает всяких связей с топологической алгеброй, хотя, учитывая всю историю проективной геометрии, можно надеяться, что топологизация основных объектов, изучаемых проективной алгеброй, явится источником новых содержательных исследований.

Написана книга в общем достаточно четко. Ее чтение будет, тем не менее, нелегким делом как ввиду сложности самого материала, так и благодаря своеобразной манере изложения. Во всех сочинениях Бэра, в том числе и в этой книге, формулировки теорем имеют, как правило, следующий вид: при таких-то общих предположениях эквивалентны такие-то утверждения. Этих утверждений приводится иногда очень много, причем лишь некоторые связи между ними действительно представляют интерес и необходимы для дальнейшего; читатель принужден, однако, с одинаковым вниманием продумывать все части доказательства теоремы.

Отмеченные недостатки не помешают книге Бэра найти достаточно широкий круг читателей. Ее прочтет всякий алгебраист, так как специалист и в теории групп, и в теории колец и алгебр, и в теории структур найдет в ней материал, близкий к его личным научным интересам. Эту книгу прочтет и каждый геометр, и если сначала он будет несколько озадачен теми изменениями, которые испытала привычная ему классическая ветвь геометрии, то затем с удовольствием обнаружит, что при этих изменениях ничего не утерялось из того, что делало эту науку близкой его сердцу. Наконец, с этой книгой ознакомится каждый математик, интересующийся разви-

тием своей науки в целом и не желающий пропустить явления, которое, при всем исключительном богатстве математики нашего времени новыми крупными явлениями, несомненно найдет отражение в будущей истории математики двадцатого века.

* * *

Перевод настоящей книги снабжен рядом примечаний с целью облегчить понимание некоторых недостаточно четко написанных мест. Выправлены также многочисленные опечатки в формулах, замеченные в оригинале.

Ссылки на литературу были сделаны автором в указателях к главам I и VII и к добавлению M, а в остальном разбросаны по всей книге. В переводе эти последние собраны в указатель, помещенный в конце книги, и несколько пополнены, причем добавления, сделанные переводчиком, отмечены звездочкой. Весь перевод книги был прочитан мною в рукописи.

А. Курош.

Ноябрь 1954 г.

ИЗ ПРЕДИСЛОВИЯ АВТОРА

В настоящей книге мы намерены показать, что проективная геометрия и линейная алгебра по существу тождественны. Конечно, тождественность этих двух дисциплин уже давно осознана. Доказательство этого утверждения содержится в ряде теорем, показывающих, что определенные геометрические понятия могут быть представлены в алгебраическом виде. Однако указанные основные теоремы существования, несмотря на всю их важность и полезность, довольно трудно найти в литературе. Поэтому основное содержание нашей книги будут составлять как раз теоремы такого типа. Эти теоремы связаны с представлением проективных геометрий линейными многообразиями, проективных отображений — полулинейными формами, коллинеаций — линейными формами и дуальных отображений — полубилинейными формами. С помощью указанных теорем мы сможем восстановить геометрию, являющуюся отправным пунктом нашего исследования, из таких на вид чисто алгебраических объектов, как кольцо эндоморфизмов исходного линейного многообразия или полная линейная группа.

Ограничения на размерность линейных многообразий будут налагаться только тогда, когда они необходимы для справедливости рассматриваемых теорем. Так, например, хорошо известно, что многие из упомянутых теорем существования перестают быть верными, если размерность очень мала. Таким образом, из наших рассмотрений будут довольно часто исключаться линейные многообразия слишком малой размерности. В то же время конечность размерности мы будем предполагать лишь в исключительных случаях; это приведет нас к установлению ряда критериев конечности линейного многообразия. Равным образом, не налагая заранее никаких ограничений на основное тело, мы получим некоторые критерии его коммутативности; все эти критерии коммутативности основного тела упомянуты в указателе. Лишь со случаем, когда основное тело имеет

характеристику 2, мы будем обращаться несколько бесцеремонно; этот случай исключается из наших рассмотрений всякий раз, когда он может вызвать затруднения.

Из сказанного в предыдущем абзаце можно сделать заключение, что в настоящей книге не появятся некоторые понятия, обычные для линейной алгебры. Исключаются из рассмотрения определители, поскольку существование определителей, обладающих всеми желательными свойствами, предполагает коммутативность основного тела. Совершенно незначительное внимание уделено матрицам; это объясняется главным образом тем, что им действительно нет места в нашем рассмотрении. Существенно лишь инвариантное содержание понятий линейного преобразования и билинейной формы, а всякое представление их матрицами означало бы ничем не оправданное фиксирование некоторой системы координат, нисколько не отличающейся от остальных систем координат.

Из наших рассмотрений исключается понятие непрерывности, несмотря на довольно большие возможности, возникающие при взаимодействии алгебраических и топологических понятий. Основатели проективной геометрии рассматривали ее, однако, как теорию пересечений и объединений, являющихся чисто алгебраическими понятиями. Мы считаем поэтому естественным ограничение наших исследований алгебраическими объектами и хотим показать, как далеко можно продвинуться, используя чисто алгебраические методы.

Некоторые параграфы этой книги имеют название «Добавление», поскольку рассматриваемые в них вопросы не относятся к основной теме нашего исследования. В добавлениях мы либо рассматриваем применения полученных нами результатов к специальным проблемам, представляющим частный интерес, либо исследуем частные случаи общей теории, для которых можно получить более глубокие результаты. Последующее изложение на эти параграфы не опирается, так что читатель может, по своему усмотрению, их пропускать.

Для чтения книги не требуется больших познаний. Мы предполагаем, что читатель знаком с такими основными алгебраическими понятиями, как группа, тело и гомоморфизм. Тем не менее все необходимые для нас алгебраические сведения, как правило, будут сообщаться, причем в такой форме, которая наиболее удобна для их использования. Мы широко используем трансфинитные методы теории

множеств — никакие метафизические предубеждения не смогут удержать автора от следования по единственно возможному пути для полного выяснения ситуации. Для удобства читателя, не знакомого с этой теорией, все те понятия и принципы теории множеств, которыми мы будем пользоваться, собраны в специальном добавлении, помещенном в конце книги. Никаких доказательств в этом добавлении не приводится; читатель может найти их в рекомендуемой литературе.

В книге нет специально выделенных упражнений. Многие утверждения приводятся, однако, без доказательств. Восполнение отсутствующих доказательств явится для читателя хорошей проверкой его знаний.

Ссылки предназначаются почти исключительно для «дополнительного чтения», которое должно либо дополнить излагаемый нами материал, либо восполнить опущенный. Мы не стараемся указывать точное происхождение каждого понятия и результата. Излагаемое в настоящей книге является в сущности достижением целого поколения алгебраистов, вдохновленных Дедекиндом, Гильбертом и Эмми Нетер; специалисту в рассматриваемой области математики будет, повидимому, ясно, что немногое добавлено автором к работам его предшественников.

Р. Бэр.

Февраль 1952 г.

ГЛАВА I

ВВЕДЕНИЕ

Целью этой вводной главы является изложение хорошо известных геометрических понятий и фактов с точки зрения современной алгебры. Мы установим некоторые важные связи между геометрическими и алгебраическими объектами. Эти связи подготовят введение в следующей главе двух основных понятий, а именно линейного многообразия и структуры его подпространств. Все другие понятия будут базироваться на них, и введение каждого нового понятия будет мотивироваться соображениями, основанными на материале этой вводной главы.

Содержание настоящей главы служит только целям иллюстрации и установления связи более специальных математических понятий с общеизвестными областями математики. Мы рассмотрим поэтому те геометрические объекты, которые соответствуют этим целям. Читатель, которому известно, что линейная алгебра по существу тождественна с аффинной и проективной геометриями, может эту главу пропустить.

Мы приводим краткий список вводных работ, в которых подчеркивается взаимная связь линейной алгебры и геометрии.

Бибербах (Bieberbach L.), Analytische Geometrie, Leipzig, Berlin, 1930;
Projektive Geometrie, Leipzig, Berlin, 1930.

Биркгоф и Мак-Лейн (Birkhoff G. and MacLane S.), A Survey of Modern Algebra, New York, 1948.

Блашке (Blaschke W.), Projektive Geometrie, Wolfenbüttel, 1948.

Мак-Даффи (MacDuffee C. C.), Vectors and Matrices, Carus Mathematical Monographs, 7, Ithaka, 1943.

Сегре (Segre B.), Lezioni di geometria moderna, v. I, Fondamenti die geometria sopra un corpo qualsiasi, Bologna, 1948.

Халмош (Halmos P.), Finite Dimensional Vector Spaces, Ann. Math. Studies, 7, Princeton, 1940.

Хефтер и Кёлер (Hefftter L. and Köhler C.), Lehrbuch der analytischen Geometrie, Bd. 1, 2, Karlsruhe, Leipzig, 1929.

Ходж и Пидо (Hodge W. V. D. and Pedoe D.), Методы алгебраической геометрии, т. 1, М., 1954. Шрейер и Шпернер (Schreier O. und Sperner E.), Einführung in die analytische Geometrie und Algebra, Bd. 1, 2, Leipzig, Berlin, 1931—1935[1]).

[1]) Том 1 имеется в русском переводе, см. Шрейер и Шпернер, Введение в линейную алгебру в геометрическом изложении, т. 1, М.—Л., 1934.—*Прим. перев.*

§ 1. Трехмерное аффинное пространство как прототип линейных многообразий

Трехмерное действительное аффинное пространство можно определить как множество E (или E_3) всех троек (x, y, z) действительных чисел x, y, z. Это краткое определение имеет тот существенный недостаток, что оно отдает предпочтение некоторой фиксированной системе координат; указанный дефект будет в свое время устранен.

Тройки чисел (x, y, z) обычно называют точками трехмерного пространства. Кроме точек, мы будем рассматривать прямые и плоскости, но, придерживаясь аффинной точки зрения, мы не будем рассматривать таких понятий, как расстояние или величина угла. Плоскость обычно определяется как совокупность точек (x, y, z), удовлетворяющих линейному уравнению

$$xa + yb + zc + d = 0,$$

где a, b, c, d — действительные числа и по крайней мере одно из чисел a, b, c отлично от 0; прямую можно определить как пересечение двух различных пересекающихся плоскостей. Известно, что точки прямой, так же как и точки плоскости, можно представить в так называемой параметрической форме, и в наших рассуждениях нам будет удобнее исходить из таких параметрических представлений. В параметрической форме точки прямой L можно представить в следующем виде:

$$L: \begin{cases} x = tu + a, \\ y = tv + b, \\ z = tw + c, \end{cases}$$

где (a, b, c) — некоторая точка прямой L, (u, v, w) — тройка действительных чисел, по крайней мере одно из которых отлично от 0, а параметр t пробегает все действительные числа. Когда t пробегает все действительные числа, точка $(tu + a, tv + b, tw + c)$ пробегает всю прямую L. Для сокращения записи положим $(a, b, c) = P$ и $(u, v, w) = D$; тогда можно записать

$$(tu + a, tv + b, tw + c) = tD + P.$$

Введем две алгебраические операции: сложение троек по правилу

$$(x, y, z) + (x', y', z') = (x + x', y + y', z + z')$$

и (скалярное) умножение тройки на действительное число по правилу

$$t(x, y, z) = (tx, ty, tz).$$

Обозначая через $R(x, y, z)$ всю совокупность троек вида $t(x, y, z)$, мы можем представить множество точек прямой L, иначе говоря прямую L, в виде

$$L = RD + P.$$

Пользуясь введенными операциями, можно подобным же образом задавать и плоскости. Пусть даны три тройки $P = (a, b, c)$, $D' = (u', v', w')$ и $D'' = (u'', v'', w'')$. Тогда множество N точек вида

$$t'D' + t''D'' + P,$$

где параметры t' и t'' пробегают независимо друг от друга все действительные числа, можно представить в виде

$$N = RD' + RD'' + P.$$

Если обе тройки D' и D'' являются 0-тройками [$D' = D'' = (0, 0, 0) = 0$], то N вырождается в точку P; если только одна из этих троек нулевая, а другая не нулевая, то N вырождается в прямую. Более обще: N является прямой, если тройка D' кратна тройке D'' или тройка D'' кратна тройке D' и по крайней мере одна из этих троек отлична от 0. Если же N — не точка и не прямая, то N представляет собой множество всех точек плоскости, другими словами, N является плоскостью.

При таком задании прямых и плоскостей мы можем рассматривать прямую $L = RD + P$ как прямую, определяемую двумя различными точками P и $P + D$, через которые она проходит, и плоскость $N = RD' + RD'' + P$ как плоскость, порождаемую тремя неколлинеарными точками P, $P + D'$, $P + D''$. Возникает вопрос, при каких условиях две пары точек определяют одну и ту же прямую; аналогично, при каких условиях две тройки неколлинеарных точек порождают одну и ту же плоскость. Можно поставить и более общий вопрос, как охарактеризовать внутренними свойствами множество всех точек прямой или плоскости.

Для ответа на эти вопросы введем следующее

Определение. Непустое множество S точек пространства E называется *семейством*, если точка $sU - sV + W$ принадлежит S всякий раз, когда s — действительное число, а точки U, V, W принадлежат S.

Заметим, что

$$s(u, u', u'') - s(v, v', v'') + (w, w', w'') =$$
$$= (su - sv + w, su' - sv' + w', su'' - sv'' + w'').$$

Множество, состоящее из одной точки, конечно, обладает этим свойством; читатель легко может убедиться, что прямые и плоскости также представляют собой семейства точек. Очевидно, что

семейством является и совокупность всех точек пространства E. Покажем теперь, что произвольное семейство точек S является или точкой, или прямой, или плоскостью, или совпадает со всем пространством E. Действительно, семейство точек S содержит по крайней мере одну точку P. Если P — единственная точка в S, то наше утверждение справедливо. Предположим поэтому, что S содержит вторую точку Q. Тогда, по определению семейства точек, S содержит всю прямую

$$L = P + R(P - Q);$$

заметим, что $P - Q \neq (0, 0, 0)$. Если этой прямой исчерпывается все S, то мы опять достигли нашей цели. Поэтому мы можем предположить, что S содержит по крайней мере одну точку K, не принадлежащую L. Но тогда, по свойству семейства точек, S содержит множество точек

$$N = P + R(Q - P) + R(K - P),$$

которое является плоскостью, поскольку точка K не принадлежит прямой L. Если S совпадает с этой плоскостью, то и на этот раз наше утверждение справедливо. Если же в S существует точка M, не принадлежащая N, то можно доказать, что семейство точек S совпадает со всем пространством E (принимая во внимание, что четыре точки P, Q, K, M «линейно независимы», а поэтому каждая другая точка от них «зависит»); детали доказательства мы оставляем читателю.

Теперь мы можем выделить те свойства пространства E, которые не зависят от системы координат. Пространство E состоит из элементов, называемых точками. Эти точки можно складывать и вычитать $(P \pm Q)$, и они относительно сложения образуют абелеву группу. Определено также скалярное умножение rP действительного числа r на точку P со свойствами

$$(r + s)P = rP + sP, \quad r(P + Q) = rP + rQ,$$
$$(rs)P = r(sP), \quad 1P = P.$$

Кроме того, выделены некоторые множества точек, называемые семействами; они характеризуются следующим свойством:

Если U, V, W — точки семейства S и если r — действительное число, то в S содержится точка $rU - rV + W$.

Аффинную геометрию можно определить (несколько предварительно) как науку о семействах точек пространства E.

Среди семейств точек особенно интересны те, которые содержат нулевую точку (нулевой элемент относительно сложения точек). Легко видеть, что множество точек S тогда и только тогда является семейством, содержащим нулевую точку, когда

(а) S содержит $P + Q$ и $P - Q$, если в S содержатся P и Q, и

(б) S содержит rP, если r — действительное число и точка P принадлежит S.

Другими словами, семейства, содержащие нулевую точку, являются как раз теми подмножествами пространства E, которые замкнуты относительно сложения, вычитания и умножения на действительные числа; как говорят, они являются подпространствами пространства E.

Если T – подпространство пространства E (т. е. подмножество, замкнутое относительно сложения, вычитания и умножения на действительные числа) и если P — точка, то множество точек $T+P$ является семейством. Если S — семейство, то совокупность T всех точек вида $P-Q$, где P и Q – точки из S, является подпространством и S можно представить в виде $S=T+P$ при произвольной точке P из S. Это показывает, что нам будут известны все семейства точек пространства E, если мы будем знать все его подпространства, т. е. изучение множества всех семейств точек пространства E можно свести к изучению множества подпространств пространства E. Совокупность же прямых и плоскостей трехмерного аффинного пространства, проходящих через нулевую точку (начало координат), имеет по существу то же самое строение, что и действительная проективная плоскость; это утверждение мы докажем в следующем параграфе.

§ 2. Действительная проективная плоскость как прототип структуры подпространств линейного многообразия

Начнем с формулировки следующего определения действительной проективной плоскости, преимуществом которого является краткость и согласованность с общепринятой терминологией. Недостаток этого определения состоит в том, что оно выделяет некоторую фиксированную систему координат.

Каждая тройка (x_0, x_1, x_2) действительных чисел, из которых не все равны 0, определяет точку, и каждую точку можно представить в таком виде.

Тройки (x_0, x_1, x_2) и (y_0, y_1, y_2) тогда и только тогда определяют одну и ту же точку, когда существует такое число $c \neq 0$, что $x_i = cy_i$ для $i = 0, 1, 2$.

Каждая тройка (u_0, u_1, u_2) действительных чисел, из которых не все равны 0, определяет прямую, и каждую прямую можно представить в таком виде.

Тройки (u_0, u_1, u_2) и (v_0, v_1, v_2) тогда и только тогда определяют одну и ту же прямую, когда существует такое число $d \neq 0$, что $u_i = v_i d$ для $i = 0, 1, 2$.

Точка, представленная в виде (x_0, x_1, x_2), тогда и только тогда принадлежит прямой, представленной в виде (u_0, u_1, u_2), когда

$$x_0u_0 + x_1u_1 + x_2u_2 = 0.$$

Если применить обозначения, подобные использованным в § 1[1]), то можно сказать, что тройки x и y определяют одну и ту же точку тогда и только тогда, когда $x = cy$, и что тройки u и v определяют одну и ту же прямую тогда и только тогда, когда $u = vd$. Основания для записи скалярного множителя d справа станут ясны позднее (гл. II, § 3); сейчас же мы только скажем, что некоторые из наших формул при такой записи будут выглядеть несколько лучше. Если мы определим скалярное произведение троек x и u по формуле

$$xu = \sum_{i=0}^{2} x_i u_i,$$

то отношение инцидентности «точка x принадлежит прямой u» будет выражаться равенством $xu = 0$. Заметим, что из равенства $xu = 0$ следуют равенства $(cx)u = 0$ и $x(ud) = 0$.

Если x — тройка, отличная от 0, то совокупность троек cx, $c \neq 0$, определяет одну и ту же точку, и поэтому мы можем сказать, не боясь недоразумения, что Rx является точкой. Аналогично, совокупность троек uR можно назвать прямой, если только тройка u отлична от 0.

Таким образом, точка Rx представляет собой множество троек, замкнутое относительно сложения и умножения на действительные числа. Если uR — прямая, то обозначим через S совокупность всех таких троек x, что $xu = 0$. Очевидно, что совокупность троек S также замкнута относительно сложения и умножения на действительные числа и что S составлена из всех точек Rx прямой uR. Мы можем поэтому отождествить прямую uR с множеством S.

Но множество всех троек $x = (x_0, x_1, x_2)$ является как раз тем трехмерным аффинным пространством, которое мы рассматривали в § 1, а точки Rx и прямые S, рассматриваемые в настоящем параграфе, являются подпространствами этого трехмерного аффинного пространства. То, что все подпространства пространства E, кроме 0 и E, являются либо точками, либо прямыми в этом проективном смысле, читатель сумеет проверить без больших усилий. Если он это сделает, то поймет обоснованность нашего утверждения, приведенного в конце предыдущего параграфа.

Таким образом, действительная проективная плоскость по существу тождественна системе подпространств (семейств с нулевой точкой) трехмерного действительного аффинного пространства.

Следовательно, все наше алгебраическое рассмотрение линейных многообразий, которое мы начинаем со следующей главы, допускает две существенно различные геометрические интерпретации: аффинную интерпретацию, в которой исходными объектами

[1]) При ссылках на материал другого параграфа той же главы будет указываться только номер параграфа. — *Прим. перев.*

являются элементы линейного многообразия (часто называемые векторами), и проективную интерпретацию, в которой исходными объектами являются подпространства. Мы будем использовать обе интерпретации, применяя каждый раз ту, которая более подходит при изучении данного конкретного вопроса, но обычно мы будем отдавать предпочтение проективной точке зрения.

Трехмерное действительное аффинное пространство и действительная проективная плоскость являются двумя важными частными примерами общих построений, к которым можно прийти посредством обобщения указанных примеров в двух направлениях. При первом отбрасываются всякие ограничения на размерность, так что для размерности рассматриваемых пространств допускаются произвольные конечные и бесконечные значения (хотя иногда мы будем исключать из наших рассмотрений пространства очень малых размерностей); при втором поле действительных чисел как основное поле заменяется любым телом – конечным или бесконечным, коммутативным или некоммутативным. Но при изучении всех этих обобщений читатель должен представлять себе ту геометрическую картину, которую мы стремились показать в этой вводной главе.

ГЛАВА II

ОСНОВНЫЕ СВОЙСТВА ЛИНЕЙНОГО МНОГООБРАЗИЯ

Материал этой главы является основой всего последующего изложения. Понятиями, введенными здесь, и теоремами, о них доказываемыми, мы будем пользоваться на протяжении всей книги. В этой главе мы докажем, что в линейном многообразии имеет место принцип дополнения; докажем существование базиса пространства, содержащего базис данного подпространства; покажем, что любые два базиса пространства состоят из одного и того же числа элементов — это число (конечное или бесконечное) есть ранг пространства. Затем легко получим основные соотношения для рангов, которые содержат как частный случай теорию систем линейных однородных уравнений (см. добавление I) и связывают ранг пространства с рангом сопряженного пространства (пространства гиперплоскостей).

§ 1. Закон Дедекинда и принцип дополнения

Линейным многообразием (F, A) называется аддитивная абелева группа A, имеющая тело F областью операторов; другими словами, определена операция умножения элементов тела F на элементы группы A. Эта операция подчинена следующим правилам:

(а) Если f — элемент из F и a — элемент из A, то их произведение fa является однозначно определенным элементом из A.

(б) $(f'+f'')a=f'a+f''a$, $f(a'+a'')=fa'+fa''$ для f, f', f'' из F и a, a', a'' из A.

(в) $1a=a$ для каждого элемента a группы A (где через 1 обозначен единичный элемент тела F).

(г) $(f'f'')a=f'(f''a)$ для f', f'' из F и a из A.

Из этих правил легко получить такие свойства:

(д) $0a=f0=0$ для f из F и a из A (где первый 0 является нулевым элементом тела F, тогда как второй и третий 0 обозначают нулевой элемент группы A).

(е) $(-f)a=f(-a)=-fa$ для f из F и a из A.

Напомним, что телом называется множество, содержащее по крайней мере два элемента, в котором определены две операции — сложение и умножение. Относительно сложения тело является абелевой группой; элементы тела, отличные от 0, образуют группу,

не обязательно коммутативную, относительно умножения; сложение и умножение связаны дистрибутивными законами[1]). Хорошим примером некоммутативного тела являются действительные кватернионы[2]).

В приведенном определении линейного многообразия мы имеем два основных класса элементов: элементы аддитивной группы A (векторы) и элементы тела F (скаляры). Чтобы различать эти два класса элементов, мы часто будем называть элементы тела F «числами из F»; такая терминология представляется оправданной тем фактом, что числа из тела F можно складывать, вычитать, умножать и делить.

Вместо выражения «линейное многообразие (F, A)» мы будем часто употреблять выражение *F-пространство A* и иногда будем говорить, что F является основным телом пространства A. Заметим, что в литературе используются также термины: *F-группа A*, *F-модуль A*, *векторное пространство A над телом F*.

Линейным подмногообразием или *подпространством* линейного многообразия (F, A) называется непустое подмножество S элементов F-пространства A, удовлетворяющее следующим требованиям:

(ж) Если S содержит элементы s' и s'', то в S содержится элемент $s' - s''$; если S содержит элемент s, а f есть число из F, то в S содержится элемент fs.

Если X, Y — произвольные подмножества элементов F-пространства A и G — произвольное подмножество чисел тела F, то, как обычно, через $X+Y$, $X-Y$ и GX мы будем обозначать соответственно множества всех сумм $x+y$, всех разностей $x-y$ и всех произведений gx, где x берется из X, y из Y и g из G. Легко проверить эквивалентность условий (ж) следующим условиям:

$$S = S+S = S-S = FS.$$

Приведем несколько примеров линейных подмногообразий: 0; точки Fp, $p \neq 0$; прямые $Fp+Fq$, где Fp и Fq — различные точки; плоскости $L+Fp$, где L — прямая и Fp — точка, не принадлежащая L. Оправдание этих терминов, помимо соображений, уже приведенных в главе I, будет дано в следующем параграфе.

Вместо термина «линейное подмногообразие» можно также использовать термины *подпространство F-пространства*, *F-подгруппа и допустимая подгруппа*.

Основным объектом изучения является для нас совокупность подпространств данного линейного многообразия. Для изучения

---

[1]) Наряду с преимущественно употребляемым в нашей литературе термином «тело», отдельные авторы употребляют также термины «кольцо с делением», «поле», «косое поле». В оригинале настоящей книги использован термин «поле». Мы, однако, *полем будем называть только коммутативное тело. — Прим. перев.*

[2]) См., например, Курош А. Г. [1], стр. 321—322. — *Прим. перев.*

строения этой совокупности рассмотрим соотношения, связывающие между собой подпространства.

Включение. Если S и T — подпространства F-пространства A и если каждый элемент из S принадлежит T, то мы будем писать $S \leqslant T$ и говорить, что S является частью T, или что S предшествует T, или что S содержится в T. Если $S \leqslant T$, но $S \neq T$, то будем писать $S < T$. Если подпространство H содержит подпространство K, а K содержит подпространство L, то будем говорить, что K «расположено между» H и L.

Пересечение. Если S и T — подпространства F-пространства A, то через $S \cap T$ обозначается множество всех таких элементов, которые принадлежат одновременно и S и T. Легко видеть, что $S \cap T$ также является подпространством.

Если Φ — некоторое множество подпространств F-пространства A, то пересечение подпространств, содержащихся в Φ, определяется как совокупность всех элементов, принадлежащих каждому подпространству множества Φ. Пересечение подпространств, содержащихся в Φ, также является подпространством; его обозначают различными способами. Например, если множество Φ состоит из конечного числа подпространств $S_1, \ldots, S_n$, то их пересечение обозначается через $S_1 \cap \ldots \cap S_n$; если Φ задается в виде $\Phi = [\ldots S_\sigma \ldots]$, то пересечение подпространств из множества Φ обозначается через $\prod_\sigma S_\sigma$, и т. д.

Сумма. Если S и T — подпространства F-пространства A, то их сумма $S + T$ определяется как множество всех элементов вида $s + t$, где s берется из S и t из T. Легко проверить, что $S + T$ является подпространством, которое, как говорят, «порождается» подпространствами S и T.

Если $S_1, \ldots, S_n$ — конечное множество подпространств F-пространства A, то их сумма

$$S_1 + \ldots + S_n = \sum_{i=1}^{n} S_i$$

определяется как совокупность всех элементов вида $s_1 + \ldots + s_n = \sum_{i=1}^{n} s_i$, где $s_i \in S_i$. Очевидно, что сумма $\sum_{i=1}^{n} S_i$ также является подпространством, а именно подпространством, порожденным S_i, $i = 1, \ldots, n$.

Если, наконец, Φ — произвольное множество подпространств F-пространства A, то суммой подпространств, содержащихся в Φ, является совокупность, состоящая из всех элементов вида $s_1 + \ldots + s_k$, где каждый элемент s_i принадлежит некоторому подпространству S из множества Φ. Сумма подпространств, содержащихся в Φ, также является подпространством, которое обозначают различными

способами, например $\sum_{\nu} S_\nu$. Заметим, что хотя в F-пространстве A определены суммы только конечного числа элементов, тем не менее имеет смысл понятие суммы бесконечного числа подпространств. Кроме того, легко проверить, что определение суммы конечного числа подпространств является частным случаем определения суммы подпространств, принадлежащих множеству Ф.

Пересечение и сумма подпространств F-пространства A связаны между собой, как легко проверить, следующим образом.

Сумма подпространств, принадлежащих множеству Ф, совпадает с пересечением всех подпространств, каждое из которых содержит все подпространства из Ф. Пересечение подпространств, принадлежащих множеству Ф, совпадает с суммой всех подпространств, содержащихся в каждом подпространстве из Ф.

Перейдем теперь к выводу более существенных соотношений между подпространствами линейного многообразия.

Закон Дедекинда. *Если R, S, T — подпространства F-пространства A и если $R \leqslant S$, то*

$$S \cap (R+T) = R + (S \cap T).$$

Доказательство. Так как $S \cap T \leqslant S$, $R \leqslant R+T$ и $R \leqslant S$, то

$$R + (S \cap T) \leqslant S \cap (R+T).$$

Обратно, если элемент s принадлежит $S \cap (R+T)$, то $s = r+t$, где $r \in R$ и $t \in T$. Поскольку $R \leqslant S$, $s-r$ содержится в S. Поэтому $t = s-r$ принадлежит $S \cap T$, так что $s = r+t$ принадлежит $R + (S \cap T)$. Отсюда следует, что $S \cap (R+T) \leqslant R + (S \cap T)$, и этим нужное равенство доказано.

Читатель сможет построить пример, показывающий, что вышеприведенное равенство не выполняется, вообще говоря, без предположения о том, что $R \leqslant S$.

Для формулировки следующей теоремы нам потребуются два новых понятия.

Фактор-пространство. Если M — подпространство F-пространства A, то следующим образом определим сравнение по модулю M: элементы x и y из A сравнимы по модулю M (обозначается $x \equiv y \pmod{M}$), если их разность $x-y$ принадлежит M.

Легко проверить, что свойство сравнимости по модулю M рефлексивно, симметрично и транзитивно. Поэтому F-пространство A можно разбить на непересекающиеся классы сравнимых элементов. Так как из сравнений $x \equiv y \pmod{M}$ и $x' \equiv y' \pmod{M}$ следуют сравнения $x+x' \equiv y+y' \pmod{M}$ и $x-x' \equiv y-y' \pmod{M}$, то сравнения можно складывать и вычитать. Поскольку для каждого элемента f тела F мы можем вывести из сравнения $x \equiv y \pmod{M}$ сравнение $fx \equiv fy \pmod{M}$, сравнения можно умножать на элементы тела F.

Классы сравнимых по модулю M элементов часто называют смежными классами по модулю M. Множество всех смежных классов по модулю M мы обозначим через A/M. Сложение и вычитание смежных классов по модулю M определяются соответствующими операциями над элементами из этих смежных классов. Произведение fX числа f из F на смежный класс X из A/M есть смежный класс, состоящий из всех элементов fx, где $x \in X$, если исключить случай, когда $f = 0$; в этом случае мы полагаем $fX = 0X = M = 0$. Из предыдущих рассуждений следует, что $(F, A/M)$ является линейным многообразием. Можно сказать, что F-пространство A/M получается из F-пространства A, если в последнем в качестве равенства рассматривать сравнения по модулю M. F-пространство A/M обычно называют фактор-пространством F-пространства A по модулю M.

Если подпространство S F-пространства A содержит подпространство M, то элементы множества S разбиваются на полные классы сравнимых по модулю M элементов. Можно образовать фактор-пространство S/M; легко видеть, что S/M является подпространством фактор-пространства A/M.

Обратно, пусть T — произвольное подпространство фактор-пространства A/M. Каждый элемент из T является классом сравнимых элементов F-пространства A. Обозначим через T^* множество элементов из A, каждый из которых принадлежит некоторому классу сравнимых элементов, содержащемуся в T. Легко доказывается, что множество T^* является подпространством F-пространства A, содержащим M и удовлетворяющим условию $T^*/M = T$.

Читателю следует рассмотреть пример, когда A — действительная проективная плоскость и M — некоторая ее точка[1]). В этом случае подпространствам фактор-пространства A/M соответствуют прямые плоскости A, проходящие через точку M. Таким образом, система подпространств фактор-пространства A/M имеет «структуру прямой».

Изоморфным отображением F-пространства A на F-пространство B называется такое взаимно однозначное отображение σ элементов из A на элементы из B, при котором

$$A\sigma = B, \quad (a+b)\sigma = a\sigma + b\sigma, \quad (fa)\sigma = f(a\sigma)$$

для a, b из A и f из F. Очевидно, что для изоморфного отображения σ существует обратное ему отображение σ^{-1} и что σ^{-1} является изоморфным отображением F-пространства B на F-пространство A.

---

[1]) Поскольку действительная проективная плоскость не является линейным многообразием, автор, очевидно, имеет в виду, что рассматривается трехмерное действительное аффинное пространство (система подпространств которого является действительной проективной плоскостью) и его подпространство — прямая, которой соответствует точка действительной проективной плоскости. — *Прим. перев.*

Это понятие изоморфизма может быть применено, в частности, к подпространствам и их фактор-пространствам.

Если между F-пространствами A и B можно установить изоморфное соответствие, то мы будем говорить, что A и B изоморфны, и писать $A \sim B$. Однако обычно вместо термина «изоморфное отображение» мы будем употреблять термин *линейное преобразование*. Таким образом, линейным преобразованием мы будем называть то, что в классической терминологии принято называть неособенным линейным преобразованием. Понятие линейного преобразования будет позже обобщено, когда мы введем более общее понятие полулинейного преобразования (гл. III, § 1).

Теорема об изоморфизме. *Если S и T — подпространства F-пространства A, то* $(S+T)/S \sim T/(S \cap T)$.

Доказательство. Каждый элемент x подпространства $S+T$ имеет вид $x=s+t$, где $s \in S$ и $t \in T$. Очевидно, что $x \equiv t \pmod{S}$. Поэтому каждый смежный класс X из $(S+T)/S$ содержит элементы подпространства T, и, следовательно, пересечение $X \cap T$ множеств X и T не пусто. Если элементы x' и x'' принадлежат $X \cap T$, то $x' \equiv x'' \pmod{S}$, так что элемент $x'-x''$ содержится в $S \cap T$; этим доказано, что $X \cap T$ является элементом фактор-пространства $T/(S \cap T)$.

Если Y — смежный класс из $T/(S \cap T)$, то множество $S+Y$, как легко проверить, является элементом фактор-пространства $(S+T)/S$. Поскольку

$$X = S + (X \cap T) \text{ для } X \text{ из } (S+T)/S,$$
$$Y = T \cap (S+Y) \text{ для } Y \text{ из } T/(S \cap T),$$

мы видим, что отображения $X \to X \cap T$ и $Y \to Y+S$ устанавливают взаимно обратные соответствия между $(S+T)/S$ и $T/(S \cap T)$; это, в частности, будут взаимно однозначные соответствия между этими фактор-пространствами. То, что выписанные отображения являются изоморфизмами, показывается совсем легко (проверку мы оставляем читателю). Этим завершается доказательство теоремы об изоморфизме.

Лемма. *Объединение любого упорядоченного (по включению) множества подпространств F-пространства A является подпространством.*

Доказательство. Если Φ — упорядоченное по включению множество подпространств F-пространства A и если $S \neq T$ — различные подпространства, принадлежащие Φ, то справедливо одно и только одно из двух соотношений: $S < T$ или $T < S$. Обозначим через J объединение всех подпространств, содержащихся в множестве Φ, так что элемент из A тогда и только тогда принадлежит J, когда он принадлежит по крайней мере одному подпространству S из Φ. Если элементы x и y содержатся в J, то в Φ

найдутся такие подпространства X и Y, что x принадлежит X и y принадлежит Y. Из наших предположений следует, что одно из этих подпространств содержится в другом, например $X \leqslant Y$. В таком случае элементы x, y и, следовательно, x y принадлежат Y; таким образом, элемент $x-y$ содержится в J. Если элемент x принадлежит подпространству X, то элемент fx, где f — число из F, также принадлежит X; этим показано, что J вместе с элементом x содержит элемент fx. Таким образом, множество J является подпространством.

Теорема о дополнении. *Для каждого подпространства S F-пространства A в A существует такое подпространство T, что $S \cap T = 0$ и $S + T = A$.*

Доказательство. Обозначим через Θ множество всех подпространств W F-пространства A, удовлетворяющих условию $S \cap W = 0$. Множество Θ содержит, например, 0 и, следовательно, не пусто. Если Φ — упорядоченное подмножество множества Θ, то мы можем построить, согласно предыдущей лемме, объединение J подпространств, принадлежащих Φ. Из построения ясно, что $J \cap S = 0$; в силу леммы, J является подпространством F-пространства A. Таким образом, J принадлежит к Θ. Этим мы показали, что к Θ можно применить теоретико-множественный принцип максимального элемента (см. добавление М). Поэтому в A существует такое подпространство T, что $S \cap T = 0$ и из $T < Q$, где Q — подпространство F-пространства A, следует $S \cap Q \neq 0$.

Теперь рассмотрим подпространство $S + T$. Пусть a — произвольный элемент из A, не принадлежащий T. Тогда $T < T + Fa$ и, следовательно, $S \cap (T + Fa) \neq 0$. Это пересечение содержит поэтому элемент $s \neq 0$, так что $s = t + fa$, где $t \in T$ и $f \in F$. Если бы число f равнялось 0, то элемент $s \neq 0$ должен был бы принадлежать $S \cap T = 0$, что невозможно. Поэтому $f \neq 0$. Следовательно, элемент $a = f^{-1}(s - t)$ содержится в $S + T$; этим доказано, что $S + T = A$. Таким образом, T является требуемым подпространством.

Если S и T — такие подпространства F-пространства A, что $S \cap T = 0$ и $S + T = A$, то мы будем говорить, что F-пространство A есть *прямая сумма* подпространств S и T, и писать $A = S \dotplus T$. Если F-пространство A является прямой суммой подпространств S и T, то подпространство T называется *дополнением* подпространства S в A. Из теоремы об изоморфизме следует, что $A/S = (S + T)/S \sim T/(S \cap T) = T$, и поэтому дополнение к подпространству S однозначно (с точностью до изоморфизма) определяется подпространством S и F-пространством A.

Пусть подпространство T является дополнением подпространства S в F-пространстве A и пусть $S \leqslant V$, где V — некоторое подпространство F-пространства A. Тогда, используя закон

Дедекинда, можно написать

$$V = V \cap (S + T) = S + (V \cap T).$$

В то же время очевидно, что $(V \cap T) \cap S = 0$. Следовательно, $V = S + (V \cap T)$. Таким образом, мы получили

Следствие. *Если подпространство S F-пространства A есть часть подпространства V и если T является дополнением S в A, то $V \cap T$ будет дополнением S в V.*

Основной результат этого параграфа можно сформулировать следующим образом: совокупность подпространств линейного многообразия (F, A) является полной дедекиндовой структурой с дополнениями. Здесь мы пользуемся обычным языком теории структур (см., например, Биркгоф [1]).

§ 2. Линейная зависимость и независимость; ранг

Конечное множество элементов $b_1, \ldots, b_n$ F-пространства A обычно называется линейно независимым, если из равенства $\sum_{i=1}^{n} f_i b_i = 0$ (где f_i — числа из F) следует, что $f_1 = \ldots = f_n = 0$. Из этого определения, в частности, следует, что элементы линейно независимого множества попарно различны.

Подмножество B F-пространства A называется *линейно независимым*, если линейно независимо (в указанном выше смысле) каждое его конечное подмножество; в противном случае подмножество B называется *линейно зависимым*. Таким образом, подмножество B линейно зависимо, если в нем существует конечное число таких попарно различных элементов $b_1, \ldots, b_n$, что $\sum_{i=1}^{n} f_i b_i = 0$, где $f_1, \ldots, f_n$ — числа тела F, по крайней мере одно из которых отлично от 0.

Пусть D — некоторое подмножество F-пространства A. Образуем сумму $\{D\} = \sum Fd$ (где суммирование распространяется на все элементы d из D); мы будем говорить, что каждый элемент получаемого таким образом подпространства $\{D\}$ *линейно зависит от подмножества D*.

Лемма 1. *Подмножество L F-пространства A тогда и только тогда линейно независимо, когда в нем нет ни одного элемента, линейно зависящего от остальных элементов из L.*

Доказательство. Если подмножество L линейно зависимо, то в нем существуют такие попарно различные элементы $b_1, \ldots, b_n$, что $\sum_{i=1}^{n} f_i b_i = 0$, где $f_1, \ldots, f_n$ — числа из F, по крайней мере одно из которых отлично от 0. Без ущерба для общности мы можем

предположить, что $f_1 \neq 0$; в таком случае

$$b_1 = \sum_{i=2}^{n} (-f_1^{-1} f_i)\, b_i,$$

так что b_1 линейно зависит от $b_2, \ldots, b_n$ и, следовательно, от элементов подмножества L, отличных от b_1. Обратное утверждение доказываемой леммы является очевидным.

Подобным же образом, даже еще проще, можно доказать, что элемент x тогда и только тогда линейно зависит от линейно независимого множества B, когда или x содержится в B, или же объединение $[B, x]$ является линейно зависимым множеством.

Базисом F-пространства A называется такое его линейно независимое подмножество, от которого линейно зависит каждый элемент из A.

Лемма 2. *Если B есть базис F-пространства A, то каждый элемент a из A можно однозначно представить в виде*

$$a = \sum_{b \in B} a(b)\, b,$$

где $a(b)$ — элементы тела F, из которых лишь конечное число отлично от 0.

Лемма почти непосредственно следует из наших определений. Для ее доказательства достаточно принять во внимание, что множество $\sum_{b \in B} Fb$ состоит из всех элементов вида $\sum_{b \in B} f(b)\, b$, где лишь конечное число элементов $f(b)$ тела F отлично от 0, и что из равенства $\sum_{b \in B} f'(b)\, b = \sum_{b \in B} f''(b)\, b$ вытекает линейное соотношение

$$\sum_{b \in B} [f'(b) - f''(b)]\, b = 0.$$

Теорема существования. *Каждое линейное многообразие обладает базисом.*

Доказательство. Предположим, что F-пространство A не нулевое (для нулевого линейного многообразия базисом является пустое множество). Тогда в A линейно независимо каждое подмножество, состоящее из одного элемента, отличного от 0. Следовательно, множество Θ всех линейно независимых подмножеств F-пространства A не пусто. Если Φ — упорядоченное (по включению) подмножество множества Θ, то построим объединение J всех подмножеств, содержащихся в Φ. Допустим, что для конечного числа элементов $b_1, \ldots, b_n$ из J выполняется равенство $\sum_{i=1}^{n} f_i b_i = 0$, где $f_1, \ldots, f_n$ — некоторые числа из F. Каждый элемент b_i содержится в некотором подмножестве B_i, принадлежащем Φ. Так как множество Φ упорядочено (по включению), то существует

такой индекс m, что $B_i \leqslant B_m$ для $i = 1, \ldots, n$. Но в таком случае элементы $b_1, \ldots, b_n$ содержатся в линейно независимом подмножестве B_m и, следовательно, $f_1 = \ldots = f_n = 0$. Таким образом, множество J линейно независимо. Теперь мы можем применить к Θ теоретико-множественный принцип максимального элемента (см. добавление М), в силу которого в Θ существует линейно независимое множество B, не содержащееся ни в каком другом линейно независимом множестве.

Пусть теперь элемент a F-пространства A не принадлежит B. Тогда множество $[B, a]$ является линейно зависимым и, как следует из сделанного выше замечания, элемент a линейно зависит от B. Таким образом, множество B является базисом F-пространства A, что и требовалось доказать.

Теорема единственности. *Любые два базиса линейного многообразия содержат одно и то же число элементов.*

Как обычно в теории множеств, мы говорим, что два множества содержат одно и то же число элементов, если между ними можно установить взаимно однозначное соответствие (см. добавление М).

Нам удобно предпослать доказательству сформулированной теоремы доказательство следующего ее частного случая, которое можно провести методом индукции.

($E.n$) *Если линейное многообразие обладает базисом, состоящим из n элементов, то и каждый его базис содержит точно n элементов* (где n — натуральное число).

Действительно, если F-пространство A обладает базисом, состоящим из одного элемента, то $A = Fb$ для некоторого $b \neq 0$ и справедливость утверждения ($E.1$) очевидна. Поэтому можно предположить, что $n > 1$ и что утверждения ($E.i$) справедливы для каждого $i < n$.

Пусть теперь F-пространство A обладает базисом, состоящим из n элементов $b_1, \ldots, b_n$, и пусть B — другой базис того же пространства. Тогда

$$\sum_{i=1}^{n-1} Fb_i < \sum_{i=1}^{n} Fb_i = A = \sum_{b} Fb,$$

где b пробегает все элементы базиса B. Поэтому невозможно, чтобы каждый элемент b из B содержался в подпространстве

$$S = \sum_{i=1}^{n-1} Fb_i.$$

Обозначим через w некоторый элемент базиса B, не принадлежащий S. Тогда, как легко видеть, элементы $b_1, \ldots, b_{n-1}, w$ образуют линейно независимое множество, ибо в противном случае элемент w содержался бы в S. Из теоремы об изоморфизме

следует, что $A/S=(S+Fb_n)/S\sim Fb_n/(Fb_n\cap S)=Fb_n$. Но Fb_n не содержит ни одного подпространства, отличного от 0 и Fb_n. Поэтому подпространство S не содержится ни в каком другом подпространстве, отличном от A. Поскольку $S<S+Fw\leqslant A$, этим показано, что $A=S+Fw$. Отсюда следует, что n элементов $b_1, \ldots, b_{n-1}, w$ образуют базис W F-пространства A.

Рассмотрим фактор-пространство A/Fw. Обозначим через x^* смежный класс по модулю Fw, содержащий элемент x из A. Легко видеть, что из равенства $\sum_{i=1}^{n-1} f_i b_i^*=0^*$ следует равенство $\sum_{i=1}^{n-1} f_i b_i=fw$; отсюда, принимая во внимание линейную независимость множества W, мы получаем, что $f_1=\ldots=f_{n-1}=0$. Поэтому элементы $b_1^*, \ldots, b_{n-1}^*$ составляют базис фактор-пространства A/Fw. Обозначим теперь через B^* множество элементов вида t^*, где t пробегает все элементы базиса B, отличные от w. Легко проверить, что B^* также является базисом фактор-пространства A/Fw. Поскольку, по индуктивному предположению, в A/Fw справедливо утверждение $(E.n-1)$, множество B^* состоит из $n-1$ элементов. Отсюда, учитывая построение множества B^*, мы получаем, что базис B состоит точно из n элементов. Таким образом, индуктивное доказательство утверждения $(E.n)$ закончено.

Доказательство теоремы единственности в общем случае. Пусть множества B' и B'' являются базисами F-пространства A. Если хотя бы одно из них, например B', состоит из конечного числа n элементов, то из утверждения $(E.n)$ следует, что B'' также содержит n элементов. Поэтому достаточно рассмотреть случай, когда оба базиса B' и B'' бесконечны. (Теоретико-множественные факты, используемые в последующем доказательстве, содержатся в добавлении М.)

Пусть T — конечное подмножество элементов базиса B'. Построим множество

$$T^{**}=B''\cap\sum_{t\in T}Ft.$$

По теореме о дополнении, в F-пространстве $\sum_{t\in T}Ft$ существует дополнение C к подпространству $\sum_{t\in T^{**}}Ft$. Добавляя к линейно независимому множеству T^{**} базис подпространства C, мы получим базис всего F-пространства $\sum_{t\in T}Ft$. Но так как это F-пространство обладает конечным базисом T, то и все его базисы конечны. Отсюда следует, что множество T^{**} конечно и содержит не больше элементов, чем множество T. Таким образом, можно установить однозначное отображение $T\to T^{**}$ множества Φ' всех конечных

подмножеств базиса B' на подмножество Θ' множества Φ'' всех конечных подмножеств базиса B''. Если w — некоторый элемент, принадлежащий B'', то в B' существует такое конечное множество элементов $b_1, \ldots, b_k$, что w содержится в $\sum_{i=1}^{k} Fb_i$. Следовательно, если обозначить через W множество элементов $b_1, \ldots, b_k$, то множество W^{**} будет содержать элемент w. Это показывает, что объединение всех подмножеств, содержащихся в Θ', совпадает со всем базисом B''.

Так как базис B' бесконечен, то он содержит столько же элементов, сколько их содержит множество Φ'. Но $T \to T^{**}$ является однозначным отображением множества Φ' на множество Θ'; поэтому множество Θ' содержит не больше элементов, чем их содержится в Φ', а потому не больше, чем в B'. В то же время, поскольку объединение всех конечных подмножеств, принадлежащих Θ', совпадает с бесконечным множеством B'', множества Θ' и B'' состоят из одного и того же числа элементов. Отсюда вытекает, что базис B'' содержит не больше элементов, чем базис B'. Но теперь из соображений симметрии следует, что и число элементов в B' не больше числа элементов в B''. Таким образом, базисы B' и B'' содержат одно и то же число элементов, чем и завершается доказательство теоремы единственности.

Историческая справка. Первая теорема такого типа была доказана Е. Штейницем (инвариантность степени трансцендентности); доказательство теоремы единственности, которое мы привели, принадлежит С. Бохнеру.

Однозначно определенное число элементов, содержащихся в каждом базисе F-пространства A, называется *рангом* $r(A)$ этого пространства. Если ранг $r(A)$ конечен, то число $r(A) - 1 = \dim A$ называется *размерностью* F-пространства A.

Структурная теорема. *F-пространства A и B изоморфны тогда и только тогда, когда совпадают их ранги, $r(A) = r(B)$. Для каждого тела F и любого кардинального числа c существует одно и, с точностью до изоморфизма, только одно F-пространство ранга c.*

Доказательство. Очевидно, что изоморфные F-пространства имеют одинаковые ранги, ибо при изоморфном отображении образом базиса является базис. Обратно, пусть F-пространства A и B имеют один и тот же ранг c. Тогда A и B обладают соответственно базисами A' и B', число элементов в каждом из которых равно c. Следовательно, существует взаимно однозначное отображение τ множества A' на множество B'. Если теперь x – элемент из A, то, по лемме 2, его можно однозначно представить в виде

$$x = \sum_{t \in A'} x(t)\, t,$$

где $x(t)$ — элементы тела F, из которых лишь конечное число отлично от 0. Положим[1])

$$x^{\sigma} = \sum_{t \in A'} x(t)\, t^{\tau};$$

легко проверить, что σ является изоморфным отображением F-пространства A на F-пространство B, индуцирующим на A' отображение τ.

Для построения F-пространства A ранга c возьмем сначала произвольное множество C символов, содержащее точно c элементов. Конструируемое F-пространство A будет состоять из всех однозначных отображений (функций) $f(v)$ множества C в тело F, удовлетворяющих следующему условию:

(+) Лишь конечное множество элементов из C отображается данной функцией f не на 0.

Если в совокупности A таких функций определить сложение по правилу

$$(f' + f'')(v) = f'(v) + f''(v) \text{ для каждого } v \text{ из } C$$

и умножение функции f на число y тела F по правилу

$$(yf)(v) = y[f(v)] \text{ для каждого } v \text{ из } C,$$

то, очевидно, A станет F-пространством.

Если w — некоторый фиксированный элемент множества C, то определим функцию f_w следующим образом:

$$f_w(v) = \begin{cases} 1 & \text{для } v = w, \\ 0 & \text{для } v \neq w. \end{cases}$$

Поскольку функции типа f_w удовлетворяют условию (+), они содержатся в A. Легко проверить, что эти функции образуют базис F-пространства A. Так как множество функций f_w и множество C содержат одно и то же число элементов, то $r(A) = c$, что и требовалось доказать.

При рассмотрении предыдущего построения читатель вспомнит, вероятно, такой пример функционального пространства, как система всех действительных функций действительного переменного.

Если кардинальное число c конечно (в этом случае мы будем обозначать его через n), то, как легко проверить, F-пространство ранга n можно построить следующим образом: элементами F-пространства будут все n-строки $(x_1, \ldots, x_n)$ с координатами x_i из тела F; сложение, вычитание и умножение на числа из F определяются «покоординатно».

---

[1]) Образ элемента x при отображении σ здесь обозначается через x^{σ}. См. добавление М, стр. 383. — *Прим. перев.*

Общая формула для ранга. *Если S и T — подпространства линейного многообразия (F, A), то*

$$r(S+T)=r(S\cap T)+r(S/S\cap T)+r(T/S\cap T).$$

Доказательство. Из теоремы о дополнении следует существование таких подпространств U и V, что $S=(S\cap T)\dot{+}U$ и $T=(S\cap T)\dot{+}V$. В силу теоремы об изоморфизме (§ 1), $U\sim S/(S\cap T)$, и поэтому $r(U)=r(S/S\cap T)$. Подобным же образом $r(V)=r(T/S\cap T)$. Заметим теперь, что $S+T=(S\cap T)\dot{+}U\dot{+}V$; следовательно, базис подпространства $S+T$ можно построить, объединив базисы подпространств $S\cap T$, U и V. Поэтому

$$r(S+T)=r(S\cap T)+r(U)+r(V)=$$
$$=r(S\cap T)+r(S/S\cap T)+r(T/S\cap T),$$

что и требовалось доказать.

Специальная формула для ранга. *Если S и T — подпространства F-пространства A, причем $S\leqslant T$, то*

$$r(T)=r(S)+r(T/S).$$

Эта формула является частным случаем предыдущей.

Формулы для рангов подпространств конечного ранга. *Если S и T — подпространства конечного ранга F-пространства A, то*

(а) *из $S\leqslant T$ и $r(S)=r(T)$ следует $S=T$;*

(б) $r(S)+r(T)=r(S\cap T)+r(S+T)$.

Доказательство. Если $S\leqslant T$ и $r(S)=r(T)$, то из условия конечности рангов этих подпространств и из специальной формулы для ранга следует, что $r(T/S)=0$. Но это равносильно тому, что $T/S=0$, или $T=S$; таким образом, предложение (а) доказано.

Чтобы доказать справедливость формулы (б), применяем к подпространствам $S\cap T$ и S специальную формулу для ранга, из которой получаем, принимая во внимание конечность рангов рассматриваемых подпространств, что $r(S/S\cap T)=r(S)-r(S\cap T)$. Подобным же образом убеждаемся, что $r(T/S\cap T)=r(T)-r(S\cap T)$. Используя эти соотношения и общую формулу для ранга, мы имеем

$$r(S+T)=r(S\cap T)+r(S/S\cap T)+r(T/S\cap T)=$$
$$=r(S)+r(T)-r(S\cap T),$$

чем и завершается доказательство формулы (б).

Формула для рангов подпространств бесконечного ранга. *Если ранг по крайней мере одного из подпространств S и T бесконечен, то*

$$r(S+T)=\max[r(S),\ r(T)].$$

Доказательство. Без ограничения общности можно предположить, что $r(T) \leqslant r(S)$. Тогда из наших условий следует бесконечность ранга $r(S)$. В силу специальной формулы для ранга, $r(T/S \cap T) \leqslant r(T)$; учитывая это, мы из общей и специальной формул для ранга, а также из «закона поглощения» для сложения бесконечных кардинальных чисел (см. добавление М), получаем, что

$$r(S+T) = r(S \cap T) + r(S/S \cap T) + r(T/S \cap T) = \\ = r(S) + r(T/S \cap T) = r(S) = \max[r(S), r(T)].$$

Замечание. Из формулы для рангов подпространств бесконечного ранга и закона поглощения для бесконечных кардинальных чисел легко вывести справедливость формулы (б) в самом общем случае. Читателю предлагается рассмотреть проблему определения ранга суммы бесконечного множества подпространств.

Теперь, когда мы приписали каждому линейному многообразию определенный ранг, можно ввести обычные геометрические наименования для пространств и подпространств некоторых специальных рангов. Так, *точками*, *прямыми* и *плоскостями* мы назовем соответственно пространства 1-го, 2-го и 3-го ранга. Поскольку рассматриваемые нами пространства могут быть и бесконечного ранга, нельзя определить гиперплоскость как такое подпространство H F-пространства A, ранг которого удовлетворяет равенству $r(A) = r(H) + 1$ (ибо в случае, когда F-пространство A имеет бесконечный ранг, оно само удовлетворяет этому условию). Мы можем, однако, определить *гиперплоскость* как такое подпространство H F-пространства A, фактор-пространство A/H по которому имеет ранг 1 (т. е. является точкой).

Из формул для ранга следует, что две различные прямые, принадлежащие одной плоскости, пересекаются по точке; F-пространство A порождается любой гиперплоскостью H вместе с произвольным подпространством S, не содержащимся в H. Заметим, кроме того, что если H' и H'' — различные гиперплоскости, то $A/(H' \cap H'')$ является прямой.

Сформулируем утверждение, легко вытекающее из предыдущих теорем.

Следующие свойства линейного многообразия (F, A) *эквивалентны:*

(а) *Ранг F-пространства A конечен.*

(б) *Каждая убывающая последовательность подпространств*

$$\ldots \leqslant S_{i+1} \leqslant S_i \leqslant \ldots \leqslant S_2 \leqslant S_1$$

содержит лишь конечное число различных членов.

(в) *Каждая возрастающая последовательность подпространств*

$$S_1 \leqslant S_2 \leqslant \ldots \leqslant S_i \leqslant S_{i+1} \leqslant \ldots$$

содержит лишь конечное число различных членов.

При доказательстве структурной теоремы мы рассматривали пространство функций, удовлетворяющих условию конечности (+). В дальнейшем нам понадобится также пространство «совершенно произвольных» функций, которое определяется следующим образом.

Пусть множество «символов» C состоит из c элементов, где c – конечное или бесконечное кардинальное число, и пусть F — произвольное тело. Тогда через $[F, C]$ обозначим множество всех однозначных отображений множества C в тело F. Операции сложения и умножения на элементы тела F определим в $[F, C]$ по следующим правилам:

Если f', f'' — элементы множества $[F, C]$, то их сумма $f'+f''$ определяется равенством

$$(f'+f'')(x)=f'(x)+f''(x) \text{ для каждого } x \text{ из } C.$$

Если f — функция из $[F, C]$ и y — элемент тела F, то функция yf определяется равенством

$$(yf)(x)=y[f(x)] \text{ для каждого } x \text{ из } C.$$

Нетрудно проверить, что множество $[F, C]$ после введения в нем вышеуказанных операций превращается в F-пространство. Очевидно, что структура этого F-пространства зависит только от числа c и не зависит от природы символов, из которых образовано множество C. Это становится еще более ясным из структурной теоремы и следующего предложения.

Предложение. (а) *Если c — конечное число, то $c=r([F, C])$.*

(б) *Если c — бесконечное кардинальное число и d — число элементов тела F, то $d^c=r([F, C])$.*

Для доказательства предложения (а) достаточно проверить, что в случае конечности числа c множество функций $\{f_x\}$, где

$$f_x(y)=\begin{cases} 1 \text{ для } y=x, \\ 0 \text{ для каждого } y\neq x,\ y\in C, \end{cases}$$

является базисом F-пространства $[F, C]$. Проверку этого утверждения мы оставляем читателю.

Прежде чем доказывать предложение (б), докажем несколько лемм. Некоторые из них представляют самостоятельный интерес. [Доказательство предложения (б) в основном опирается на теорию множеств. Поэтому читателю, не знакомому с этой теорией, советуем при первом чтении книги опустить доказательство предложения (б).]

Лемма 3. *Если F-пространство A имеет бесконечный ранг и если число элементов тела F равно d, то A содержит $dr(A)$ элементов.*

Доказательство. Пусть B — некоторый базис F-пространства A. Тогда B содержит $r(A)$ элементов, и каждый элемент из

A можно однозначно представить в виде

$$w = \sum_{b \in B} w(b) b, \qquad (*)$$

где $w(b)$ — числа из F, из которых лишь конечное число отлично от 0.

Обозначим через d^* число элементов тела F, отличных от 0; тогда $d = d^* + 1$. Если $b_1, \ldots, b_k$ — конечное множество различных элементов, принадлежащих базису B, то A содержит точно d^{*k} элементов вида $\sum_{i=1}^{k} w_i b_i$, где w_i — числа из F, отличные от 0. Так как бесконечное множество B состоит из $r(A)$ элементов, то для каждого целого положительного k число различных подмножеств, состоящих из k элементов базиса B, равно $r(A)$. Рассмотрим теперь все элементы F-пространства A, имеющие в представлении (*) точно k отличных от 0 коэффициентов. Из предыдущих рассуждений следует, что число таких элементов равно $d^{*k} r(A)$. Поэтому число всех элементов F-пространства A равно $\sum_k d^{*k} r(A)$.

Случай 1. Если d — конечное число, то d^* и d^{*k} — также конечные числа и, в силу бесконечности ранга $r(A)$, справедливо равенство $r(A) = d^{*k} r(A)$. Следовательно,

$$\sum_k d^{*k} r(A) = \sum_k r(A) = r(A)\, \aleph_0 = r(A) = r(A)\, d.$$

Случай 2. Если d — бесконечное кардинальное число, то $d = d^* = d^{*k}$ и поэтому

$$\sum_k d^{*k} r(A) = \sum_k d\, r(A) = d\, r(A)\, \aleph_0 = d\, r(A);$$

тем самым наша лемма полностью доказана.

Лемма 4. *Если c — бесконечное кардинальное число и d — число элементов тела F, то число элементов F-пространства $[F, C]$ равно $dr([F, C]) = d^c$.*

Доказательство. Поскольку c — бесконечное кардинальное число, легко проверить, что ранг F-пространства $[F, C]$ также бесконечен. Например, множество функций f_x вида

$$f_x(y) = \begin{cases} 1 \text{ для } y = x, \\ 0 \text{ для } y \neq x, \ y \in C, \end{cases}$$

линейно независимо в $[F, C]$ и содержит c элементов; следовательно, $c \leqslant r([F, C])$. Поэтому мы можем воспользоваться леммой 3, в силу которой F-пространство $[F, C]$ содержит $dr([F, C])$ элементов.

С другой стороны, так как $[F, C]$ есть множество всех однозначных отображений множества C, состоящего из c элементов,

в множество F, имеющее d элементов, то оно содержит d^c элементов; это следует из определения кардинального числа d^c. Таким образом, $dr([F, C]) = d^c$, чем и завершается доказательство леммы.

Доказательство предложения (б) в случае $d < d^c$. В этом случае равенство $r([F, C]) = d^c$ справедливо потому, что из $d < d^c$ и $r([F, C]) < d^c$ следовало бы, что $dr([F, C]) < d^c$, но последнее неравенство противоречит лемме 4.

Таким образом, нам остается рассмотреть случай, когда $d = d^c$. В этом случае, поскольку кардинальное число c бесконечно и $1 < d$, бесконечно и кардинальное число d. Докажем теперь следующую лемму.

Лемма 5. *Если тело F состоит из d элементов, где d — бесконечное кардинальное число, и если A есть F-пространство конечного ранга n, то в A существует такое подмножество W, содержащее d элементов, что произвольные n элементов, принадлежащие W, линейно независимы.*

Доказательство. Рассмотрим множество Θ всех подмножеств T F-пространства A, удовлетворяющих условию:

(T. n) Произвольные n элементов, принадлежащие T, линейно независимы.

Если, например, $b_1, \ldots, b_n$ составляют базис F-пространства A, то это множество элементов содержится в Θ; заметим, кроме того, что множество $b_1, \ldots, b_n, \sum_{i=1}^{n} b_i$, состоящее из $n+1$ элементов, также содержится в Θ. Если Φ — упорядоченное по включению подмножество множества Θ, то возьмем объединение J всех множеств, принадлежащих Φ. Если $j_1, \ldots, j_n$ — любые n различных элементов из J, то каждый из них содержится в некотором множестве, принадлежащем Φ. Если j_i содержится в множестве S_i, принадлежащем к Φ, то, ввиду упорядоченности по включению множества Φ, существует такой индекс m, что $0 < m \leqslant n$ и $S_i \leqslant S_m$ для $i = 1, \ldots, n$. Поэтому все j_i содержатся в S_m. Но S_m удовлетворяет условию (T. n), в силу которого элементы $j_1, \ldots, j_n$ линейно независимы. Таким образом, объединение J само удовлетворяет условию (T. n). Этим мы показали, что к множеству Θ можно применить теоретико-множественный принцип максимального элемента (см. добавление М). Поэтому в A существует подмножество W, обладающее следующими свойствами:

(а) W содержит по крайней мере $n+1$ элемент.

(б) Любые n элементов, принадлежащие W, линейно независимы.

(в) Если W является подмножеством множества W', удовлетворяющего условию (T. n), то $W = W'$.

(То, что W можно считать обладающим свойством (а), следует из сделанного выше замечания о том, что Θ содержит по крайней мере одно множество, состоящее из $n+1$ элементов.)

Допустим, что число элементов множества W меньше d; обозначим тогда через W' множество всех $(n-1)$-строк[1]) элементов из W. Пусть t' — число всех $(n-1)$-строк, из которых состоит множество W'. Покажем, что

(1) $1 < n < t' < d$.

Эти включения безусловно справедливы в (невозможном) случае, когда t' является конечным числом; если же t' — бесконечное кардинальное число, то t' совпадает с числом элементов множества W [ибо число подмножеств, состоящих из одного и того же конечного числа элементов бесконечного множества, равно числу элементов этого бесконечного множества (см. добавление M)].

(2) t' совпадает с числом подпространств, каждое из которых порождается $(n-1)$-строкой, содержащейся в W'.

Заметим прежде всего, что каждая $(n-1)$-строка, принадлежащая W', в силу свойства (б), линейно независима; следовательно, каждая $(n-1)$-строка из W' порождает в F-пространстве A подпространство ранга $n-1$. Если $h_1, \ldots, h_{n-1}$ и $k_1, \ldots, k_{n-1}$ — две $(n-1)$-строки из W', порождающие одно и то же подпространство, то каждое k_i линейно зависит от $h_1, \ldots, h_{n-1}$. Поэтому, если хотя бы один из элементов $k_1, \ldots, k_{n-1}$, например k_1, был бы отличен от всех h_i, то n различных элементов $h_1, \ldots, h_{n-1}$, k_1 множества W были бы линейно зависимыми, что противоречит свойству (б). Таким образом, различные $(n-1)$-строки, содержащиеся в W', порождают различные подпространства F-пространства A; этим утверждение (2) доказано.

(3) Если S — подпространство ранга i и если $i > 1$, то число подпространств ранга $i-1$, содержащихся в S, не меньше d.

Обозначим через $s_1, \ldots, s_i$ некоторый базис подпространства S. Если x — элемент тела F, то положим

$$S_x = \sum_{j=1}^{i-2} Fs_j + F(s_{i-1} + xs_i).$$

Легко видеть, что $r(S_x) = i-1$ и что $S_x = S_y$ тогда и только тогда, когда $x = y$ (нужно принять во внимание, что элементы s_j линейно независимы). Таким образом, мы построили d различных подпространств ранга $i-1$, содержащихся в S. (Поскольку d — бесконечное кардинальное число, нетрудно доказать, что число всех таких подпространств точно равно d.)

Обозначим теперь через W'' множество всех подпространств F-пространства A, порождаемых $(n-1)$-строками из W'. В силу утверждения (2), число подпространств, принадлежащих W'', равно t'.

[1]) Под $(n-1)$-строками здесь автор понимает подмножества, состоящие из $n-1$ попарно различных элементов.— *Прим. перев.*

(4) Если $0 < i < n$, то в A существует подпространство V_i ранга $n-i$, не содержащееся ни в одном подпространстве, принадлежащем множеству W''.

Из утверждения (3) следует, что в F-пространстве A существует не меньше d подпространств ранга $n-1$; в то же время из утверждений (1) и (2) вытекает, что число подпространств, принадлежащих множеству W'', меньше d. Поэтому в A существует по крайней мере одно подпространство V_1 ранга $n-1$, не принадлежащее W''; тем самым утверждение (4) доказано для случая, когда $i=1$. Предположим теперь, что утверждение (4) уже доказано для некоторого i, удовлетворяющего условию $0 < i < n-1$. Тогда в A существует такое подпространство V_i ранга $n-i$, которое не содержится ни в одном из подпространств, принадлежащих W''. Поэтому, если H — произвольное подпространство, принадлежащее W'', то $H < H+V_i \leqslant A$; следовательно,

$$n-1=r(H)<r(H+V_i)\leqslant r(A)=n, \quad \text{откуда} \quad r(H+V_i)=n=r(A)$$

и, в силу формулы для ранга (а), $H+V_i=A$. Используя теперь формулу для ранга (б), мы получаем, что

$$n-1+n-i=r(H)+r(V_i)=$$
$$=r(H+V_i)+r(H\cap V_i)=n+r(H\cap V_i),$$

или

$$r(H\cap V_i)=n-i-1.$$

Поскольку число всех подпространств вида $H\cap V_i$, где H лежит в W'', меньше d и так как, в силу утверждения (3), число всех подпространств ранга $n-i-1$, содержащихся в V_i, не меньше d, то существует подпространство V_{i+1} ранга $n-(i+1)$, содержащееся в V_i и отличное от всех пересечений $H\cap V_i$ подпространства V_i с подпространствами H, принадлежащими W''. Очевидно, что V_{i+1} не может быть частью никакого подпространства H множества W'', ибо в противном случае оно совпало бы с одним из подпространств вида $H\cap V_i$. Проведенная индукция доказывает утверждение (4).

(5) В A существует такой элемент v, который не содержится ни в одном из подпространств H, принадлежащих W''.

Утверждение (5) является частным случаем утверждения (4), когда $i=n-1$.

Рассмотрим теперь множество M, полученное добавлением к множеству W элемента v, о котором говорилось в утверждении (5). Из свойства (б) множества W и утверждения (5) следует, что M удовлетворяет условию ($T.$ n) (ибо в противном случае элемент v содержался бы в одном из подпространств H, принадлежащих W''). Но $W < M$, что противоречит свойству (в). Таким образом, предполагая, что число элементов множества W меньше d, мы

пришли к противоречию. Так как d — бесконечное кардинальное число, то само F-пространство A состоит из d элементов, и, следовательно, число элементов множества W должно равняться d. Тем самым наша лемма полностью доказана.

Лемма 6. *Если C есть множество всех натуральных чисел и если число d элементов тела F бесконечно, то $d \leqslant r([F, C])$.*

Доказательство. Обозначим через A_n F-пространство ранга n, а через

$$b\left[\tfrac{1}{2}n(n-1)+1\right], \ldots, b\left[\tfrac{1}{2}n(n+1)\right]$$

— его базис. В силу леммы 5, в A_n существует такое подмножество V_n, состоящее из d элементов, что n произвольных элементов из V_n линейно независимы. Так как множества F и V_n содержат одно и то же число элементов, то существует взаимно однозначное отображение σ_n тела F на множество V_n. Если теперь x — элемент тела F, то он отображается на элемент x^{σ_n}, который можно представить в виде

$$x^{\sigma_n} = x\left[\tfrac{1}{2}n(n-1)+1\right] b\left[\tfrac{1}{2}n(n-1)+1\right] + \ldots + x\left[\tfrac{1}{2}n(n+1)\right] b\left[\tfrac{1}{2}n(n+1)\right],$$

где коэффициенты $x[i]$ являются однозначно определенными элементами тела F. Таким образом, $x[i]$ принадлежит F для каждого x из F и каждого натурального числа i[1]). Поэтому каждое $x[i]$ можно рассматривать как однозначное отображение множества C натуральных чисел в тело F. Следовательно, каждое $x[i]$ является элементом F-пространства $[F, C]$. Предположим теперь, что в $[F, C]$ для некоторых попарно различных элементов $x_1, \ldots, x_n$ тела F имеет место равенство $\sum_{j=1}^{n} f_j x_j[i] = 0$, где $f_1, \ldots, f_n$ — элементы из F. Но это эквивалентно тому, что в теле F справедливы равенства

$$\sum_{j=1}^{n} f_j x_j[i] = 0 \text{ для } i = 1, \ldots.$$

Отсюда следует, что

$$\sum_{j=1}^{n} f_j x_j^{\sigma_n} = \sum_{j=1}^{n} f_j \sum_{i} x_j[i] b[i] = \sum_{i}\left[\sum_{j=1}^{n} f_j x_j[i]\right] b[i] = 0,$$

где сумма по i берется от $i = n(n-1)/2+1$ до $i = n(n+1)/2$. Но $x_j^{\sigma_n}$ являются n попарно различными элементами множества

[1]) Если одновременно рассматривать F-пространства A_n при всех n. — *Прим. перев.*

V_n, и поэтому они линейно независимы. Следовательно, $f_1 = \ldots = f_n = 0$.

Таким образом, мы показали, что множество элементов $x[i]$ F-пространства $[F, C]$ линейно независимо. Но это множество состоит из такого же числа элементов, что и тело F. Отсюда следует, что ранг F-пространства $[F, C]$ не меньше d, что и требовалось доказать.

Доказательство предложения (б) в случае $d = d^c$. Так как кардинальное число c бесконечно, то множество C содержит счетное подмножество C^*. Совокупность всех функций f из $[F, C]$, удовлетворяющих условию $f(x) = 0$ для x из C, не принадлежащих подмножеству C^*, является подпространством F-пространства $[F, C]$, изоморфным, очевидно, F-пространству $[F, C^*]$. Поскольку $d = d^c$, из бесконечности кардинального числа c следует бесконечность кардинального числа d. Поэтому мы можем воспользоваться леммой 6[1]), в силу которой ранг F-пространства $[F, C^*]$ не меньше d. Отсюда вытекает, что

$$d \leqslant r([F, C]).$$

С другой стороны, в силу леммы 4, число всех элементов F-пространства $[F, C]$ равно $d^c = d$ и поэтому ранг $r([F, C])$ не может быть больше d. Следовательно, $r([F, C]) = d = d^c$, чем и завершается доказательство предложения (б).

Следствие. *$r([F, C]) = c$ тогда и только тогда, когда число c конечно.*

Это утверждение непосредственно следует из только что доказанного предложения, поскольку для бесконечного кардинального числа c имеют место хорошо известные из теории множеств неравенства

$$c < 2^c \leqslant d^c,$$

так как каждое тело содержит по крайней мере два элемента.

§ 3. Сопряженное пространство

Линейной формой над F-пространством A называется однозначное отображение f элементов a из A на элементы af из F, удовлетворяющее условиям

$$(a' + a'')f = a'f + a''f \text{ для } a', a'' \text{ из } A,$$

$$(xa)f = x(af) \text{ для } x \text{ из } F \text{ и } a \text{ из } A.$$

Такая запись линейных форм аналогична записи скалярных произведений (a на f). В то же время обычная функциональная запись

[1]) Здесь автор использует тот очевидный факт, что пространство всех функций, рассматриваемых на множестве целых положительных чисел, изоморфно пространству всех функций, определенных на произвольном счетном множестве. — *Прим. перев.*

линейных форм (линейный функционал $f(x)$ вместо произведения xf) имеет некоторые неудобства, возникающие при определении умножения (см. ниже). Заметим, например, что «ассоциативный закон» $(xa)f = x(af)$ при функциональной записи имел бы вид $f(xa) = xf(a)$.

Совокупность всех линейных форм над A мы обозначим через $L(A)$. В $L(A)$ следующим образом определим *сложение*: если f' и f'' — линейные формы над A, то $f' + f''$ является отображением A в F, определяемым равенством

$$a(f' + f'') = af' + af'' \text{ для каждого } a \text{ из } A.$$

Легко проверить, что сумма (а также разность) линейных форм является линейной формой и что $L(A)$ относительно определенного сложения будет *абелевой группой*.

Определим теперь *умножение* линейных форм на элементы тела F.

Если f — линейная форма над A и x — элемент тела F, то fx является отображением A в F, задаваемым равенством

$$a(fx) = (af)x \text{ для каждого } a \text{ из } A.$$

Так как элементы af и x оба принадлежат телу F, то легко видеть, что fx также является линейной формой над A. Заметим, что, в то время как элементы из A умножаются на элементы тела F слева, линейные формы умножаются на элементы тела F справа.

Сложение линейных форм и умножение линейной формы на элементы тела F обладают следующими свойствами.

(а′) Если $f \in L(A)$ и $x \in F$, то их произведение fx является однозначно определенным элементом из $L(A)$.

(б′) $(f' + f'')x = f'x + f''x$, $f(x' + x'') = fx' + fx''$ для f, f', f'' из $L(A)$ и x, x', x'' из F.

(в′) $f1 = f$ для f из $L(A)$ (через 1 обозначен единичный элемент тела F).

(г′) $f(x'x'') = (fx')x''$ для f из $L(A)$ и x', x'' из F.

Все четыре свойства доказываются достаточно просто, так что мы предоставляем сделать это читателю. (Выписанные формулы подтверждают целесообразность выбранной нами записи произведения линейной формы f на число x из F в виде символа fx вместо символа xf. Если бы мы пользовались вторым обозначением, то формула (г′) имела бы вид

$$(x'x'')f = x''(x'f).$$

Читатель может найти другие примеры подобного рода.) Сравнивая свойства (а′) — (г′) с теми правилами, при помощи которых в § 1 определялось линейное многообразие (F, A), мы замечаем, что они по существу тождественны между собой и отличаются только порядком умножения на элементы тела F; это изменение

обусловлено тем, что линейные формы умножаются на элементы из F справа. Поэтому $L(A)$ также можно рассматривать как F-пространство; всякий раз, когда нам нужно будет подчеркнуть, что в этом пространстве имеет место умножение справа на элементы тела F, мы будем о нем говорить как о линейном многообразии $(L(A), F)$.

Линейное многообразие $(L(A), F)$ называется *пространством, сопряженным F-пространству A*. Очевидно, что все результаты, полученные нами для F-пространства A, остаются справедливыми и для сопряженного к A пространства $L(A)$. В частности, $L(A)$ обладает рангом, который следующим образом связан с рангом F-пространства A:

Теорема 1. (а) *Если ранг $r(A)$ конечен, то $r(A) = r[L(A)]$.*

(б) *Если ранг $r(A)$ бесконечен, то $r[L(A)] = d^{r(A)}$, где d—число элементов тела F.*

Доказательство. Обозначим через B какой-нибудь базис F-пространства A. Если f' и f'' — такие элементы сопряженного пространства $L(A)$, что $bf' = bf''$ для каждого b из B, то, используя основные свойства линейных форм, легко вывести равенство $f' = f''$. В то же время, если произвольным образом сопоставить каждому элементу b из B элемент $v(b)$ из F, то можно определить такую линейную форму f, что $bf = v(b)$ для каждого b из B. Она определяется следующим образом:

$$\left[\sum_{b \in B} w(b)\, b\right] f = \sum_{b \in B} w(b)\, v(b);$$

напомним, что каждый раз лишь конечное число коэффициентов $w(b)$ отлично от 0 (см. лемму 2, § 2). Отсюда видно, что $L(A)$ по существу тождественно с F-пространством всех однозначных отображений множества B в тело F (если определить в последнем умножение на элементы из F справа); наша теорема непосредственно вытекает теперь из предложения, доказанного в § 2.

Следствие 1. *Ранг линейного многообразия тогда и только тогда равен рангу сопряженного пространства, когда он конечен.*

Это утверждение непосредственно вытекает из предыдущей теоремы (см. также § 2, стр. 39, следствие).

Следствие 2. *Два F-пространства конечного ранга тогда и только тогда изоморфны, когда изоморфны пространства, им сопряженные.*

Это утверждение непосредственно следует из того, что в случае конечности ранга F-пространства тот же ранг имеет и сопряженное ему пространство и что F-пространства одного и того же ранга изоморфны (см. структурную теорему, § 2). Для F-пространств бесконечного ранга аналогичное утверждение не имеет места, поскольку из равенства $d^{r(A)} = d^{r(B)}$ в случае, когда $r(A)$ и $r(B)$ — бесконечные кардинальные числа, вообще говоря, не следует равенство

$r(A)=r(B)$. Например, если $d=2^{2^{\aleph_0}}$, $r(A)=\aleph_0$ и $r(B)=2^{\aleph_0}$, то $d=d^{r(A)}=d^{r(B)}$.

Необходимо отметить, что из равенства рангов F-пространств A и $L(A)$ не следует их изоморфность, ибо A допускает умножение на элементы тела F слева, а $L(A)$ — справа. Если F-пространство A имеет конечный ранг n, то A можно представить в виде F-пространства всех n-строк $(a_1, \ldots, a_n)$; в таком же виде можно представить и сопряженное пространство $L(A)$. Отображая каждую n-строку $(a_1, \ldots, a_n)$, рассматриваемую как элемент из A, на ту же самую n-строку, но рассматриваемую как элемент из $L(A)$, мы, очевидно, получим изоморфное отображение аддитивной группы A на аддитивную группу $L(A)$. Однако читатель может легко убедиться, что в общем случае невозможно установить соответствующее правило, относящееся к поведению этого отображения при умножении на числа из тела F.

Из следующего замечания станет понятным, что различие между правыми и левыми пространствами на самом деле более глубокое, чем различие в способах записи произведения. Предположим, что F-пространство A допускает умножение слева на элементы основного тела F, а F-пространство B допускает умножение на элементы того же тела F справа. В таком случае кажется естественным определить между ними «изоморфизм» σ как такое изоморфное отображение аддитивной группы A на аддитивную группу B, при котором $(fa)^\sigma=a^\sigma f$ для a из A и f из F. Но тогда для любой пары чисел x, y из F и любого элемента a из A мы будем иметь

$$a^\sigma xy=(a^\sigma x)\,y=(xa)^\sigma y=[y(xa)]^\sigma=[(yx)a]^\sigma=a^\sigma yx,$$

откуда следует, что или $A=0$, или F является полем. Дальнейший анализ различий между левыми и правыми пространствами будет дан ниже в главе IV.

Некоторую замену «отсутствующего изоморфизма» между A и $L(A)$ можно получить, рассматривая пространство, сопряженное к сопряженному пространству. Линейные формы над F-пространством, допускающим умножение справа, можно определить точно так же, как определялись линейные формы над линейным многообразием, допускающим умножение слева, делая при этом очевидные изменения, обусловленные иным порядком умножения; эти линейные формы тоже образуют F-пространство. Мы без ущерба можем пользоваться одной и той же символикой для пространств, допускающих умножение слева или справа. Пусть для F-пространства A, допускающего умножение слева на элементы тела F, построено сопряженное пространство $L(A)$, допускающее умножение на элементы того же тела F справа, а для $L(A)$ построено сопряженное пространство, которое мы будем обозначать через $L[L(A)]$ или $L^2(A)$ (оно допускает умножение на элементы тела F слева). Таким образом, A и $L^2(A)$ являются F-пространствами одного и того

же типа. Установим теперь основные соотношения между A и $L^2(A)$.

Если t—элемент F-пространства A, то можно следующим образом определить линейную форму t^* над $L(A)$:

$$t^*f = tf \text{ для каждого } f \text{ из } L(A).$$

Легко проверить, что каждое t^* действительно является линейной формой над $L(A)$ и что отображение $t \longrightarrow t^*$ является изоморфизмом F-пространства A на подпространство A^* F-пространства $L^2(A)$. Такое отображение мы будем называть *естественным изоморфизмом A в $L^2(A)$*.

Теорема 2. *Естественный изоморфизм F-пространства A в F-пространство $L^2(A)$ тогда и только тогда является отображением на все $L^2(A)$, когда ранг $r(A)$ конечен.*

Доказательство. Если F-пространство A имеет конечный ранг, то, используя дважды теорему 1 (а) и изоморфность A с A^*, мы получаем, что

$$r(A^*) = r(A) = r[L(A)] = r[L^2(A)].$$

Отсюда, в силу конечности $r(A^*)$ и формулы для ранга (а), следует равенство $A^* = L^2(A)$.

Если ранг F-пространства A бесконечен, то из теоремы 1 (б) вытекает, что

$$r[L^2(A)] = d^{r[L(A)]}, \quad r[L(A)] = d^{r(A)},$$

где d — число элементов тела F. Но из теоретико-множественных соображений следует, что

$$r(A^*) = r(A) < d^{r(A)} < d^{d^{r(A)}} = r[L^2(A)],$$

и поэтому $A^* < L^2(A)$.

Замечание 1. Ввиду существования естественного изоморфизма между A и A^*, мы можем отождествить каждый элемент t из A с соответствующим ему элементом t^* из A^*. Таким образом мы отождествим A с A^*. Если ранг $r(A)$ конечен, то A отождествляется со всем $L^2(A)$ и, следовательно, в этом случае сопряженное пространство к сопряженному пространству можно считать совпадающим с исходным линейным многообразием. Именно это лежит в основе симметрии, существующей между F-пространством A и сопряженным ему пространством $L(A)$ (подробности см. в добавлении II).

СООТВЕТСТВИЕ ГАЛУА МЕЖДУ A И $L(A)$

Чтобы получить это фундаментальное и важное для дальнейшего соответствие между F-пространством A и сопряженным пространством $L(A)$, обозначим через XY, $X \leqslant A$ и $Y \leqslant L(A)$, совокупность всех элементов вида xy для x из X и y из Y.

Если T — некоторое подмножество F-пространства A, то через $E(T)$ обозначим множество всех таких линейных форм f, что $Tf=0$.

Если T — некоторое подмножество F-пространства $L(A)$, то через $S(T)$ обозначим множество всех таких элементов s из A, что $sT=0$.

Читатель легко докажет следующие важные утверждения относительно определенных таким образом операторов E и S.

$E(T)$ является подпространством F-пространства $L(A)$.

Из $T'\leqslant T''$ следует $E(T'')\leqslant E(T')$.

$$T\leqslant S[E(T)].$$
$$E(T)=ESE(T).$$
$$TE(T)=0.$$

$S(T)$ является подпространством F-пространства A.

Из $T'\leqslant T''$ следует $S(T'')\leqslant S(T')$.

$$T\leqslant E[S(T)].$$
$$S(T)=SES(T).$$
$$S(T)T=0.$$

Последние формулы выделяют важные классы подпространств F-пространств A и $L(A)$, состоящие из подпространств, представимых соответственно в виде $S(T)$ и $E(T)$. Большое значение имеет задача охарактеризовать эти подпространства в классе всех подпространств; в дальнейшем мы остановимся на этой задаче.

Предложение 1. *Если M — подпространство линейного многообразия (F, A), то $E(M)$ изоморфно $L(A/M)$ и $L(A)/E(M)$ изоморфно $L(M)$.*

Доказательство. Если линейная форма f принадлежит $E(M)$, то $Mf=0$. Если X — смежный класс из A/M, то $X=M+x$ для произвольного элемента x, содержащегося в X, и, следовательно, $Xf=(M+x)f=xf$ является однозначно определенным элементом тела F. Теперь легко проверить, что отображение X в Xf является линейной формой, которую мы обозначим через f^*, над F-пространством A/M. Если линейные формы f и g, принадлежащие $E(M)$, определяют одну и ту же линейную форму над A/M (т. е. $f^*=g^*$), то для каждого элемента x из A будет выполняться равенство

$$xf=(M+x)f=(M+x)f^*=(M+x)g^*=(M+x)g=xg,$$

из которого следует, что $f=g$. Теперь легко проверить, что отображение f из $E(M)$ на f^* из $L(A/M)$ является изоморфным отображением подпространства $E(M)$ в F-пространство $L(A/M)$. Если, наконец, h — произвольная линейная форма над A/M, то следующим образом построим линейную форму k над A, содержащуюся в $E(M)$:

$$xk=(M+x)h \text{ для каждого } x \text{ из } A.$$

Очевидно, что $k^*=h$. Следовательно, указанное выше изоморфное отображение $E(M)$ в $L(A/M)$ на самом деле является искомым изоморфным отображением $E(M)$ на $L(A/M)$.

Каждая линейная форма f над F-пространством A индуцирует линейную форму f^M над подпространством M, определяемую равенством

$$xf^M = xf \text{ для каждого } x \text{ из } M.$$

Очевидно, что $(f'+f'')^M = f'^M + f''^M$ и $(fy)^M = f^M y$ для f, f', f'' из $L(A)$ и y из F; очевидно также, что $f^M = 0$ тогда и только тогда, когда f содержится в $E(M)$. Таким образом, отображение элемента f из $L(A)$ в элемент f^M из $L(M)$ индуцирует изоморфизм факторпространства $L(A)/E(M)$ в F-пространство $L(M)$. Пусть теперь h — произвольная линейная форма над F-пространством M. В силу теоремы о дополнении (§ 1), существует такое подпространство N F-пространства A, что $A = M \dotplus N$. Линейная форма k над A, задаваемая равенством

$$xk = \begin{cases} xh & \text{для } x \text{ из } M, \\ 0 & \text{для } x \text{ из } N, \end{cases}$$

очевидно, удовлетворяет условию $k^M = h$. Следовательно, отображение f на f^M индуцирует искомый изоморфизм $L(A)/E(M)$ на все пространство $L(M)$; этим наше предложение полностью доказано.

Следствие 3. *Пусть M — подпространство F-пространства A; тогда*

$$r[L(A)] = r[L(M)] + r[L(A/M)]$$

и

$$r[E(M)] = \begin{cases} r(A/M), & \text{если ранг } r(A/M) \text{ конечен,} \\ d^{r(A/M)}, & \text{если ранг } r(A/M) \text{ бесконечен} \\ & \text{и } d \text{ — число элементов тела } F. \end{cases}$$

Это утверждение легко вывести из предыдущего предложения и теоремы 1, если вспомнить, что изоморфные линейные многообразия имеют равные ранги и что $r(A/B) + r(B) = r(A)$ для каждого подпространства B F-пространства A (см. специальную формулу для ранга, § 2).

Предложение 2. *Если M — подпространство F-пространства A, то $M = S[E(M)]$.*

Доказательство. Выше было отмечено, что $M \leqslant S[E(M)]$. Пусть теперь элемент x из A не содержится в M. Построим подпространство $M \dotplus Fx$. Заметим, что $Fx \cap M = 0$, ибо в противном случае элемент x содержался бы в подпространстве M. Применяя теорему о дополнении (§ 1) к подпространству $M \dotplus Fx$, найдем такое подпространство N F-пространства A, что $A = [M \dotplus Fx] \dotplus N$. Тогда каждый элемент a из A можно однозначно представить в виде

$$a = a' + f(a)x + a'', \quad \text{где } a' \in M, \ f(a) \in F \text{ и } a'' \in N. \qquad (*)$$

Отображение h, определяемое равенством

$$ah = f(a),$$

где a — произвольный элемент из A и $f(a)$ — его коэффициент в представлении (*), является линейной формой над A, удовлетворяющей условиям $Mh = 0$ и $xh = 1$. Эти равенства показывают, что h принадлежит $E(M)$, и поэтому x не содержится в $S[E(M)]$. Таким образом, если элемент x не содержится в M, то он не содержится и в $S[E(M)]$; тем самым доказано, что $M = S[E(M)]$.

Замечание 2. Для иллюстрации предыдущих результатов рассмотрим произвольную гиперплоскость H F-пространства A. Из определения гиперплоскости следует, что $r(A/H) = 1$. Отсюда, используя следствие 3, мы получаем, что $r[E(H)] = 1$. Таким образом, «гиперплоскость удовлетворяет ровно одному уравнению», ибо все уравнения, удовлетворяемые данной гиперплоскостью, получаются умножением одного из них на элементы основного тела. Поскольку, в силу предложения 2, $H = S[E(H)]$, гиперплоскость «определяется одним уравнением».

Предложение 3. (а) *Если ранг подпространства T сопряженного пространства $L(A)$ конечен, то $r(T) = r[A/S(T)]$.*

(б) *Следующие свойства подпространства T сопряженного пространства $L(A)$ эквивалентны:*

(I) *T имеет конечный ранг.*

(II) *$A/S(T)$ имеет конечный ранг.*

(III) *Если подпространство X сопряженного пространства $L(A)$ содержится в T, то $X = E[S(X)]$.*

(в) *Тогда и только тогда $X = E[S(X)]$ для каждого подпространства X сопряженного пространства $L(A)$, когда F-пространство A имеет конечный ранг.*

Прежде чем доказывать это предложение, докажем следующую лемму.

(3. г) *Если $f_1, \ldots, f_i$ — конечное множество элементов из $L(A)$, то*

$$r[A/S(\sum_{j=1}^{i} f_j F)] \leqslant i.$$

Доказательство. Лемма, очевидно, справедлива для $i = 0$, ибо $S(0) = A$. Предположим, что лемма уже доказана для $i - 1$, где i — некоторое положительное число. Легко проверить, что имеет место следующее равенство:

$$S(\sum_{j=1}^{i} f_j F) = S(f_1) \cap \ldots \cap S(f_i).$$

Далее заметим, что так как

$$S(\sum_{j=1}^{i} f_j F) \leqslant S(\sum_{j=1}^{i-1} f_j F),$$

то, в силу специальной формулы для ранга (§ 2),

$$r[A/S(\sum_{j=1}^{i} f_jF)]=r[A/S(\sum_{j=1}^{i-1} f_jF)]+r[S(\sum_{j=1}^{i-1} f_jF)/S(\sum_{j=1}^{i} f_jF)].$$

Но из теоремы об изоморфизме (§ 1) следует, что

$$S(\sum_{j=1}^{i-1} f_jF)/S(\sum_{j=1}^{i} f_jF)=[S(f_1)\cap\ldots\cap S(f_{i-1})]/[S(f_1)\cap\ldots\cap S(f_i)]\sim$$

$$\sim[S(\sum_{j=1}^{i-1} f_jF)+S(f_i)]/S(f_i);$$

ранг последнего F-пространства не больше 1, ибо, как нетрудно проверить, фактор-пространство $A/S(f)$ для каждого $f\neq 0$ изоморфно телу F и, следовательно, имеет ранг, равный 1. Проведенная полная индукция и доказывает лемму (3. г).

Доказательство предложения 3. Если подпространство T сопряженного пространства $L(A)$ имеет конечный ранг n, то $T=\sum_{i=1}^{n} t_iF$, где элементы $t_1, \ldots, t_n$ составляют базис подпространства T. Поэтому, в силу предыдущей леммы (3. г),

$$r[A/S(T)]\leqslant r(T) \qquad (a^*)$$

для каждого подпространства T конечного ранга сопряженного пространства $L(A)$.

Таким образом, если подпространство T сопряженного пространства $L(A)$ имеет конечный ранг, то, ввиду неравенства (а*), конечен также ранг $r[A/S(T)]$; этим показано, что из свойства (I) следует свойство (II).

Предположим теперь, что конечен ранг $r[A/S(T)]$, и рассмотрим такое подпространство X сопряженного пространства $L(A)$, что $X\leqslant T$. Тогда $S(T)\leqslant S(X)$ и, следовательно, ранг фактор-пространства $A/S(X)$ также конечен. Поскольку $X\leqslant E[S(X)]$, мы получаем, используя следствие 3, что

$$r(X)\leqslant r(E[S(X)])=r[A/S(X)].$$

Этим показано, что ранг $r(X)$ конечен, а поэтому, в силу (а*), $r[A/S(X)]\leqslant r(X)$. Следовательно, $r(X)=r[A/S(X)]=r(E[S(X)])$. Отсюда, используя конечность рангов подпространств X и $E[S(X)]$ и формулу для ранга (а) (§ 2), получаем, что $X=E[S(X)]$. Таким образом, свойство (III) следует из свойства (II). Попутно полностью доказано утверждение (а), ибо мы показали, что из конечности ранга подпространства T следует конечность ранга фактор-пространства $A/S(T)$, а из конечности $r[A/S(T)]$ следует равенство $r(T)=r[A/S(T)]$.

Допустим, наконец, что для подпространства T сопряженного пространства $L(A)$ справедливо свойство (III). Тогда, если X — произвольное подпространство, содержащееся в T, то, в силу следствия 3, $X = E[S(X)]$ может иметь либо конечный, либо несчетный ранг (ибо из $1 < d$ следует $\aleph < d^{\aleph}$; см. добавление М). Но если бы ранг подпространства T был бесконечен, то в T непременно содержалось бы подпространство счетного ранга, поскольку в бесконечном базисе всегда содержится счетное линейно независимое подмножество. Таким образом, предположение о бесконечности ранга подпространства T противоречит тому, что в T, как мы выше заметили, не может содержаться подпространство счетного ранга. Следовательно, ранг $r(T)$ конечен; тем самым мы показали, что из свойства (III) следует свойство (I), чем и завершается полное доказательство утверждения (б).

Если мы применим утверждение (б) к случаю, когда $T = L(A)$, и заметим, что, согласно предложению 2, $S[L(A)] = S[E(0)] = 0$, то увидим, что утверждение (в) непосредственно следует из (б).

При доказательстве того, что из свойства (III) следует свойство (I), мы использовали соображения такого же типа, как те, которые впервые применил Дедекинд при доказательстве невозможности получить полное соответствие Галуа для бесконечных алгебраических расширений.

Приведем другое доказательство того факта, что если ранг $r(A)$ конечен, то $X = E[S(X)]$ для каждого подпространства X сопряженного пространства $L(A)$. Действительно, из условия конечности ранга $r(A)$ и теоремы 2 следует, что A можно отождествить с $L^2(A)$. При этом оператор S, определенный на $L(A)$ со значениями в A, совпадает с оператором E, определенным на $L(A)$ со значениями в сопряженном к $L(A)$ пространстве $L^2(A)$, а оператор E, определенный на A со значениями в $L(A)$, совпадает с оператором S, определенным на $L^2(A)$ со значениями в $L(A)$. Поэтому наше утверждение непосредственно следует из предложения 2.

Обычно *дуальным отображением* называют такое взаимно однозначное отображение одного частично упорядоченного множества на некоторое другое частично упорядоченное множество, при котором отношение порядка изменяется на обратное. Система подпространств линейного многообразия является частично упорядоченным множеством относительно включения. Мы можем представить теперь основные результаты предложений 2 и 3 в следующем виде.

Теорема 3. *Если F-пространство A имеет конечный ранг, то операторы E и S индуцируют взаимно обратные дуальные отображения между частично упорядоченными множествами подпространств F-пространства A и сопряженного ему пространства $L(A)$.*

В случае, когда ранг F-пространства A конечен, из следствия 3 и симметрии между A, E и $L(A)$, S легко получается основная

Формула для ранга. *Если F-пространство A имеет конечный ранг n, то*

$$n = r(M) + r[E(M)]$$

для каждого подпространства M F-пространства A,

$$n = r(N) + r[S(N)]$$

для каждого подпространства N сопряженного пространства L(A).

(Заметим, что, в силу конечности ранга $r(A)$, $r(A/M) = r(A) - r(M)$ и $r(A) = r[L(A)]$.)

Добавление I

Применение к системам линейных однородных уравнений

Рассмотрим систему

$$\sum_{i=1}^{n} x_i a_{ik} = 0, \quad k = 1, \ldots, m, \tag{1}$$

m линейных однородных уравнений с n неизвестными x_i и с коэффициентами a_{ik} из тела F. Обозначим через S совокупность всех n-строк, каждая из которых представляет собой систему элементов $x_1, \ldots, x_n$ тела F, являющуюся решением системы уравнений (1). Легко проверить, что S обладает следующими свойствами.

Если n-строки $(x_1, \ldots, x_n)$ и $(y_1, \ldots, y_n)$ принадлежат S, то и их сумма $(x_1 + y_1, \ldots, x_n + y_n)$ принадлежит S. Вместе с n-строкой $(x_1, \ldots, x_n)$ в S содержится n-строка $(tx_1, \ldots, tx_n)$, где t — произвольный элемент тела F.

Таким образом, пользуясь понятиями, введенными в § 1, мы можем сказать, что S является подпространством F-пространства всех n-строк с координатами из тела F; условимся обозначать это F-пространство символом (F, n). Сразу же отметим, что ранг F-пространства (F, n) равен n. Подпространство S, естественно, имеет ранг $r(S)$, не превышающий n; на обычном языке теории систем линейных уравнений это означает, что все решения системы (1) можно получить из $r(S)$ независимых решений [иногда также говорят, что система (1) имеет $r(S)$ решений].

Пусть теперь $b_1, \ldots, b_m$ — произвольные элементы тела F. Тогда, как легко видеть, каждое решение системы (1) является также решением уравнения

$$\sum_{i=1}^{n} x_i \sum_{k=1}^{m} a_{ik} b_k = 0;$$

это новое уравнение «порождается» уравнениями исходной системы (1). Совокупность E всех уравнений, порождаемых исходными уравнениями, также можно рассматривать как подпространство

некоторого F-пространства ранга n, только допускающего умножение на элементы основного тела справа. Для того чтобы использовать здесь результаты § 3, сделаем следующее.

Обозначим через a_k линейную форму над F-пространством (F, n), отображающую n-строку $(x_1, \ldots, x_n) = x$ на элемент $xa_k = \sum_{i=1}^{n} x_i a_{ik}$ тела F. Легко проверить, что a_k действительно является линейной формой. Тогда то, что мы обозначили через E, будет не чем иным, как подпространством $\sum_{k=1}^{n} a_k F$ сопряженного пространства $L[(F, n)]$, а S совпадает с подпространством $S(E)$ F-пространства (F, n) (здесь использованы обозначения § 3). Так как (F, n) имеет конечный ранг n, то из результатов § 3 следует, что

$$E = E[S(E)] \text{ и } n = r(S) + r(E).$$

Другими словами, система всех уравнений, порождаемых исходными уравнениями (1), совпадает с системой всех уравнений, удовлетворяемых всеми решениями системы (1), а число n равно сумме числа независимых решений системы (1) и ранга системы всех уравнений, порождаемых уравнениями (1).

Конечно, те же самые результаты достаточно просто получаются методом исключения, т. е. исключением одного неизвестного из первого уравнения и подстановкой получающегося выражения в остальные уравнения системы, что приводит к системе, состоящей из $m - 1$ уравнений с $n - 1$ неизвестными, и т. д.

Обычное приведение системы линейных уравнений к нормальному виду можно теперь получить следующим образом. Выберем некоторый базис F-пространства (F, n), содержащий базис подпространства S. Если $s_1, \ldots, s_n$ — такой базис F-пространства (F, n) и $s_{n-k+1}, \ldots, s_n$ — базис подпространства S, то линейные формы $f_1, \ldots, f_k$, определяемые равенствами

$$s_j f_i = \begin{cases} 1, & \text{если } j = i, \\ 0, & \text{если } j \neq i, \end{cases}$$

образуют базис подпространства E. Теперь видно, что при переходе к новым неизвестным исходная система уравнений преобразуется в систему $y_i = 0$, $i = 1, \ldots, k$.

Добавление II

Спаренные пространства

Симметрия между линейным многообразием (конечного ранга) и сопряженным ему пространством станет еще более очевидной, если мы введем следующее понятие, в котором указанные два

линейных многообразия используются совершенно равноправным образом.

Пусть даны тело F, F-пространство A, допускающее умножение слева на элементы из F, и F-пространство B, допускающее умножение справа на элементы из F. Пусть, кроме того, определено произведение элементов из A на элементы из B, обладающее следующими свойствами:

(а) Для каждого элемента a из A и для каждого элемента b из B произведение ab является однозначно определенным элементом тела F.

(б) $$(a'+a'')b=a'b+a''b,\quad a(b'+b'')=ab'+ab''$$

для любых a, a', a'' из A и b, b', b'' из B.

(в) $x(ab)=(xa)b$, $(ab)x=a(bx)$ для a из A, b из B и x из F.

F-пространства A и B, связанные между собой произведением ab, обладающим перечисленными выше свойствами (а), (б), (в), называются *спаренными F-пространствами*. Спаренные F-пространства мы будем обозначать через A, B или через (B, F, A).

Из результатов § 3 следует, что F-пространство A и сопряженное ему пространство $L(A)$ составляют спаренную пару F-пространств; такую же пару F-пространств образуют второе сопряженное пространство $L^2(A)$ и сопряженное пространство $L(A)$.

Следующее почти очевидное замечание показывает, что приведенные примеры являются типичными примерами таких пар линейных многообразий.

(г) Если A, B – спаренные F-пространства и если b – фиксированный элемент из B, то отображение каждого элемента a из A на элемент ab тела F является линейной формой над A; аналогично, если a – фиксированный элемент из A, то отображение каждого элемента b из B на элемент ab тела F является линейной формой над B.

Теорема. *Следующие свойства спаренных F-пространств A, B конечного ранга эквивалентны:*

(I) *Из $Ab=0$ следует $b=0$, и из $aB=0$ следует $a=0$.*

(II) *Из $Ab=0$ следует $b=0$, и каждая линейная форма над A индуцируется некоторым элементом из B.*

(III) *Каждая линейная форма над B индуцируется некоторым элементом из A, и из $aB=0$ следует $a=0$.*

(IV) *Каждая линейная форма над A индуцируется элементом из B, и каждая линейная форма над B индуцируется элементом из A.*

Доказательство. Пусть справедливо свойство (I). Тогда, если элементы b' и b'' из B индуцируют одну и ту же линейную форму над A, то $ab'=ab''$ для каждого a из A. Отсюда $A(b'-b'')=0$ и, следовательно, $b'-b''=0$, т. е. $b'=b''$. Поэтому F-пространство B можно отождествить с подпространством линейных форм,

индуцированных элементами из B, сопряженного пространства $L(A)$. Из свойства (I) вытекает также, что $S(B)=0$, и поэтому, в силу предложения 3 (§ 3), $B=E[S(B)]=E(0)=L(A)$. Тем самым показано, что свойство (II) следует из свойства (I); подобным же образом можно показать, что из свойства (I) следует свойство (III).

Теперь докажем, что

(д) *если каждая линейная форма над A индуцируется некоторым элементом из B, то из* $aB=0$ *следует* $a=0$.

В самом деле, из $aB=0$ и нашего предположения вытекает, что a содержится в $S[L(A)]$. Но, в силу предложения 2 (§ 3), $S[L(A)]=S[E(0)]=0$, и, следовательно, $a=0$.

Из утверждения (д) непосредственно следует, что при выполнении свойства (II) выполняется и свойство (I); точно так же можно доказать, что свойство (I) справедливо, если справедливо свойство (III). Таким образом, мы убедились в эквивалентности свойств (I), (II) и (III).

Если, наконец, выполняется свойство (IV), то, в силу утверждения (д), справедливо и свойство (III). Обратно, из эквивалентных между собой свойств (II) и (III) очевидным образом следует свойство (IV). Теорема доказана.

Замечание. Отметим, что конечность рангов F-пространств A, B была использована лишь при доказательстве того, что из свойства (I) следуют свойства (II) и (III).

Следствие. *Если для спаренных F-пространств A, B конечного ранга справедливы эквивалентные между собой свойства* (I) — (IV) *(из предыдущей теоремы), то каждое из этих F-пространств является сопряженным пространством для другого, причем их ранги совпадают.*

Это утверждение следует из замечания, сделанного в процессе доказательства теоремы, и из теоремы 1 (§ 3).

§ 4. Присоединенное пространство

Если A является F-пространством, то мы получаем сопряженное ему пространство, рассматривая все линейные формы, отображающие A в F. Естественно, возникает вопрос об изучении отображений F в A; этому вопросу мы и посвятим настоящий параграф.

Линейной антиформой f называется отображение, переводящее каждый элемент x тела F в однозначно определенный элемент xf F-пространства A, удовлетворяющее следующим условиям:

(а) $(x+y)f=xf+yf$ для x, y из F;

(б) $(xy)f=x(yf)$ для x, y из F.

Если f и g — две линейные антиформы, то мы определим их сумму $f+g$ как отображение F в A, задаваемое следующим

равенством:

(в) $x(f+g)=xf+xg$ для каждого x из F.

Легко проверить, что сумма линейных антиформ также является линейной антиформой и что совокупность $\mathbf{A}=\mathbf{A}(F, A)$ всех линейных антиформ является абелевой группой относительно введенного сложения.

Если f — линейная антиформа и x — число из F, то их произведение xf определяется как отображение F в A, задаваемое равенством

(г) $y(xf)=(yx)f$ для каждого y из F.

Непосредственным подсчетом нетрудно убедиться, что произведение xf также является линейной антиформой. Теперь легко проверить, что $\mathbf{A}=\mathbf{A}(F, A)$ является F-пространством, которое мы назовем *пространством, присоединенным* к F-пространству A. Заметим, что F-пространство A и присоединенное к нему пространство оба допускают умножение слева на элементы тела F.

Теорема. *Отображение линейной антиформы f на элемент $1f$ из A (где через 1 обозначен единичный элемент тела F) является изоморфным отображением F-пространства $\mathbf{A}$ на F-пространство A.*

Доказательство. Отображение $f \longrightarrow 1f$ является, очевидно, однозначным. Далее, если $1f=1g$, то, в силу условия (б), для каждого x из F мы имеем

$$xf=(x1)f=x(1f)=x(1g)=(x1)g=xg,$$

откуда

$$f=g.$$

Таким образом, определенное нами отображение является взаимно однозначным. Если a — произвольный элемент из A, то, отображая каждое число x из F в элемент xa из A, мы получаем такую линейную антиформу f, что $1f=a$; тем самым показано, что рассматриваемое соответствие определяет взаимно однозначное отображение F-пространства $\mathbf{A}$ на все F-пространство A. Если f и g — линейные антиформы, то, по определению (в),

$$1(f+g)=1f+1g;$$

таким образом, при нашем отображении сумме элементов соответствует сумма их образов. В силу определения (г), произведению xf числа x из F на линейную антиформу f соответствует элемент

$$1(xf)=(1x)f=(x1)f=x(1f);$$

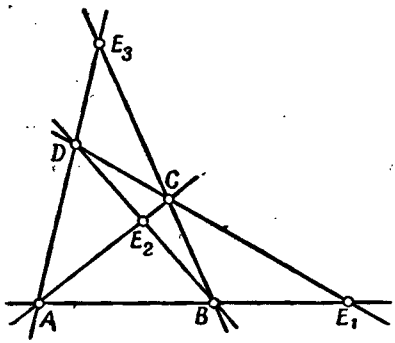
этим завершается полная проверка того, что наше отображение является изоморфным.

Изоморфизм, который мы установили между линейным многообразием и присоединенным к нему пространством, является естественным изоморфизмом; поэтому F-пространства A и $\mathfrak{A}$ по существу тождественны между собой. Этим объясняется то, что изучение присоединенного пространства вносит мало нового в теорию линейных многообразий, в то время как изучение сопряженного пространства, которое отличается по существу от исходного F-пространства, приводит к определенным результатам. Тем не менее предыдущая теорема окажется полезной для дальнейшего (см. гл. V, § 2).

Добавление III

Постулат Фано

В последующих разделах книги нам придется исключать иногда из наших рассмотрений случай, когда характеристика основного тела F равна 2 (т. е. когда $+1=-1$). Геометрическую интерпретацию этого случая можно получить следующим образом.



Фиг. 1

Будем говорить, что четыре точки A, B, C, D линейного многообразия M *образуют четырехугольник*, если они компланарны (т. е. ранг подпространства $A+B+C+D$ равен 3), но никакие три из этих точек не коллинеарны (таким образом,

$$A+B+C=A+B+D=$$
$$=A+C+D=B+C+D,$$

и ранг этого пространства равен 3). В таком случае, как следует из формулы для ранга (б) (§ 2), прямые $A+B$ и $C+D$ пересекаются в некоторой точке E_1, прямые $A+C$ и $B+D$ — в некоторой точке E_2, а прямые $A+D$ и $B+C$ — в некоторой точке E_3. Точки E_i называются диагональными точками данного четырехугольника; нетрудно проверить, что A, B, C, D, E_1, E_2, E_3 — семь различных точек.

Так называемый постулат Фано исключает возможность коллинеарности диагональных точек; наша цель состоит в том, чтобы дать алгебраическую характеристику этого геометрического постулата.

Пусть точки A, B, C и D F-пространства M образуют четырехугольник. Тогда точка $D=Fd$ принадлежит плоскости $A+B+C$ и, следовательно, существуют такие элементы a, b, c, содержащиеся соответственно в A, B, C, что $d=a+b+c$. Если бы

элемент c равнялся 0, то точка D лежала бы на прямой $A+B$, что невозможно; аналогично доказывается, что и элементы a, b отличны от 0. Поэтому

$$A=Fa,\ B=Fb,\ C=Fc.$$

Теперь точки E_i можно определить следующим образом. Так как

$$E_1=(Fa+Fb)\cap(Fc+Fd),$$

то из равенства $d=a+b+c$ следует, что $E_1=F(a+b)$. (Очевидно, что $F(a+b)\leqslant E_1$, а то, что эти подпространства совпадают, вытекает из равенства их рангов.) Подобным же образом мы можем убедиться, что $E_2=F(a+c)$ и $E_3=F(b+c)$.

Поскольку точки E_i попарно различны, они тогда и только тогда коллинеарны, когда $E_1<E_2+E_3$; но это включение имеет место тогда и только тогда, когда в теле F существуют такие числа u и v, что

$$a+b=u(a+c)+v(b+c).$$

Ввиду линейной независимости элементов a, b и c F-пространства M, выполнение предшествующего равенства эквивалентно справедливости следующих равенств:

$$1=u,\ 1=v,\ 0=u+v,\ \text{откуда}\ 0=1+1.$$

Последнее равенство означает, однако, что характеристика тела F равна 2.

Используя приведенные выше соображения, легко доказать справедливость следующего утверждения.

Если ранг F-пространства M не меньше 3, *то следующие свойства эквивалентны*:

(I) *Характеристика тела F равна* 2.

(II) *В M существует четырехугольник, диагональные точки которого коллинеарны.*

(III) *Диагональные точки каждого четырехугольника F-пространства M коллинеарны.*

ГЛАВА III

ПРОЕКТИВНЫЕ ОТОБРАЖЕНИЯ

Линейное многообразие (F, A) можно рассматривать как алгебраический фундамент проективной геометрии, образованной совокупностью подпространств F-пространства A; в частности, то, что на классическом языке называют «выбором системы координат проективной геометрии», является не чем иным, как выбором некоторого определенного базиса линейного многообразия (F, A). Для сопоставления отметим, что в то время, как исходными объектами алгебраического исследования линейного многообразия (F, A) являются элементы группы A, при проективно-геометрическом подходе к изучению линейных многообразий исходными объектами являются подпространства. В главе II у нас преобладала алгебраическая точка зрения; начиная с этой главы, в основном будет принята точка зрения проективной геометрии.

Первым вопросом, возникающим при таком переходе, является вопрос о том, какие связи существуют между алгебраическим и геометрическим строением линейного многообразия (F, A). Типичным в этом направлении является вопрос о том, будет ли основное тело F не только алгебраическим, но и проективно-геометрическим инвариантом. В настоящей главе мы дадим положительный ответ на этот вопрос в предположении, что ранг линейного многообразия (F, A) не меньше 3; представляет исторический интерес тот факт, что указанный вопрос был поставлен и решен только на протяжении последней половины или четверти столетия.

Для того чтобы изучить соотношения между алгебраическими и проективными инвариантами, нам нужно найти связь между алгебраическими изоморфными отображениями линейного многообразия (F, A), обычно известными под такими названиями, как линейные и полулинейные преобразования, и геометрическими изоморфными отображениями, так называемыми проективными отображениями. Это приведет нас к некоторым теоремам, которые будут тесно связаны с тем, что обычно называют основной теоремой проективной геометрии. Однако, так как классические исследования в основном ограничиваются изучением автопроективных отображений, притом преимущественно специального вида, то в настоящей главе появится целый ряд теорем, заменяющих указанные классические результаты.

Изучение этих вопросов при более общих предположениях читатель может найти в работе автора [2].

§ 1. Представление проективных отображений полулинейными преобразованиями

Проективным отображением линейного многообразия (F, A) *на линейное многообразие* (G, B) называется отображение σ подпространств F-пространства A на подпространства G-пространства B, обладающее следующими свойствами:

(а) Если X есть подпространство F-пространства A, то его образ $X\sigma$ является однозначно определенным подпространством G-пространства B.

(б) $X \leqslant Y$ тогда и только тогда, когда $X\sigma \leqslant Y\sigma$.

(в) $X = Y$ тогда и только тогда, когда $X\sigma = Y\sigma$.

(г) Для каждого подпространства Z G-пространства B существует (и притом только одно) такое подпространство Z' F-пространства A, что $Z'\sigma = Z$.

Другими словами, проективным отображением называется взаимно однозначное и сохраняющее отношение порядка отображение частично упорядоченного (по включению) множества всех подпространств F-пространства A на частично упорядоченное множество всех подпространств G-пространства B. Ясно, что для всякого проективного отображения существует обратное отображение и что оно также является проективным.

Свойства (а) – (г) не являются, очевидно, независимыми друг от друга. Так, свойство (в) можно вывести из свойства (б); существуют также более глубокие связи. Подчеркнем, что в определении проективного отображения основные тела F и G рассматриваемых линейных многообразий (F, A) и (G, B), вообще говоря, различны. Одна из основных наших задач состоит в том, чтобы вывести изоморфизм тел F и G, когда это возможно, из проективной эквивалентности F-пространства A и G-пространства B [1]).

Читателю полезно сравнить понятие проективного отображения с понятием изоморфного отображения (гл. II, § 1). Первое из этих понятий имеет дело только с подпространствами, и в нем совершенно не упоминается основное тело, тогда как при определении изоморфного отображения основными объектами являются элементы линейного многообразия и основного тела.

Докажем некоторые простые, но часто используемые свойства проективных отображений.

(д) При проективном отображении сохраняются пересечение и сумма подпространств.

---

[1]) Проективно эквивалентными автор называет такие линейные многообразия, между которыми можно установить проективное соответствие. См. замечание автора на стр. 71.—*Прим. перев.*

Доказательство. Если Φ есть некоторое множество подпространств линейного многообразия (F, A), то сумма S подпространств, содержащихся в Φ, характеризуется (т. е. однозначно определяется) следующими двумя свойствами:

(′) $X \leqslant S$ для каждого X из Φ;

(″) если T — такое подпространство F-пространства A, что $X \leqslant T$ для каждого X из Φ, то $S \leqslant T$.

Легко проверить, что образ $S\sigma$ обладает теми же самыми свойствами по отношению к подпространствам $X\sigma$ для X из Φ; следовательно, $S\sigma$ является суммой подпространств, содержащихся в $\Phi\sigma$. Аналогично доказывается утверждение о пересечении.

(е) $0\sigma = 0$ и $A\sigma = B$.

Это утверждение очевидно [см., например, (д)].

(ж) Точки отображаются на точки.

Это свойство следует из того, что точка является таким подпространством P, которое характеризуется следующими двумя проективно инвариантными свойствами: $P \neq 0$, и из $0 < X \leqslant P$, где X - некоторое подпространство, следует $X = P$.

Если T — некоторое линейно независимое подмножество F-пространства A, то множество точек Ft, $t \in T$, мы назовем *независимым множеством точек*. Заметим, что в случае, когда множество T линейно независимо, различные элементы t' и t'' из T определяют различные точки. Следующая лемма оправдывает выбранную терминологию и окажется полезной при последующем изложении.

Лемма 1. *Множество T элементов F-пространства A тогда и только тогда линейно независимо, когда оно удовлетворяет следующим двум условиям*:

(α) *Если t' и t'' — различные элементы множества T, то t' не содержится в подпространстве Ft''.*

(β) *Если P — точка из множества T^*, состоящего из всех точек Ft для t из T, и если P' есть сумма всех остальных точек, содержащихся в T^*, то $P \cap P' = 0$.*

Доказательство. Необходимость выполнения условия (α) в линейно независимом множестве T очевидна. Далее, если w — элемент, содержащийся в $P \cap P'$ [используются обозначения, введенные в формулировке условия (β)], то $w = xt = \sum_{i=1}^{n} x_i t_i$, где t, t_i — попарно различные элементы из T и x, x_i — числа из F. Поэтому равенство $w = 0$ непосредственно следует из линейной независимости множества T.

Обратно, если T удовлетворяет условиям (α) и (β), то, как следует из (α), все точки Ft, где $t \in T$, попарно различны. Если $\sum_{i=1}^{n} f_i t_i = 0$, где t_i — различные элементы из T и f_i — числа из F, то $f_i t_i$ для каждого $i = 1, \ldots, n$ принадлежит пересечению

$Ft_i \cap \sum_{j \neq i} Ft_j$, которое совпадает с 0 в силу условия (β). Следовательно, $f_i = 0$, и тем самым доказана линейная независимость множества T.

Замечание. Множество T, состоящее из двух отличных от 0 различных элементов t' и t'', таких, что $Ft' = Ft''$, удовлетворяет условию (β) и не удовлетворяет условию (α). Таким образом, условие (α) не может быть опущено.

Предложение 1. *При проективном отображении сохраняется ранг.*

Доказательство. Пусть σ — проективное отображение F'-пространства A' на F''-пространство A'', и пусть S — подпространство F'-пространства A'; базис подпространства S обозначим через T. T является линейно независимым подмножеством F'-пространства A'. Поэтому, в силу леммы 1, множество T^* точек $F't$, где $t \in T$, содержит столько же точек, сколько элементов содержится в T. Заметим, что S является суммой точек, принадлежащих T^*. Следовательно, и $S\sigma$ является суммой точек, принадлежащих $T^*\sigma$. Построим теперь такое множество R элементов F''-пространства A'', что каждая точка, содержащаяся в $T^*\sigma$, имеет вид $F''r$, где $r \in R$, и различные элементы из R определяют различные точки, принадлежащие $T^*\sigma$. Из леммы 1 следует, что T^* удовлетворяет условию (β). Поэтому R удовлетворяет условиям (α) и (β); отсюда, и из леммы 1 вытекает, что R линейно независимо, а потому является базисом подпространства $S\sigma$. Но множества R и T состоят из одного и того же числа элементов. Следовательно, $r(S) = r(S\sigma)$.

Нельзя утверждать, конечно, что из проективной эквивалентности линейных многообразий следует тождественность тел, над которыми они рассматриваются. В лучшем случае можно надеяться на то, что эти тела изоморфны. Последнее, как мы покажем, действительно имеет место «почти всегда». Для того чтобы это доказать, нам понадобится следующее основное понятие.

Изоморфное отображение линейного многообразия (F, A) на линейное многообразие (G, B) является, в соответствии с общепринятой алгебраической терминологией, взаимно однозначным соответствием между объединением множеств F и A и объединением множеств G и B, сохраняющим основные операции, а именно: сложение в A и в B, сложение и умножение в F и в G, умножение элементов тела F на элементы группы A и элементов тела G на элементы группы B. В связи с этим определим (следуя Сегре) *полулинейное преобразование линейного многообразия* (F, A) *на линейное многообразие* (G, B) как пару $\sigma = (\sigma', \sigma'')$, состоящую из изоморфного отображения σ' аддитивной группы A на аддитивную группу B и изоморфного отображения σ'' тела F на тело G, удовлетворяющих условию

$$(fa)^{\sigma'} = f^{\sigma''} a^{\sigma'} \text{ для } f \text{ из } F \text{ и } a \text{ из } A.$$

Заметим, что мы воспользовались записью действия преобразования в виде показателя степени, которая нагляднее, чем запись в виде множителя. Далее, едва ли возникнут недоразумения, если мы одним и тем же символом σ будем обозначать изоморфное отображение σ' группы A на группу B и изоморфное отображение σ'' тела F на тело G. При таком обозначении приведенная выше формула, связывающая отображения σ' и σ'', примет более простой вид $(fa)^\sigma = f^\sigma a^\sigma$. Полулинейное преобразование σ называется *линейным преобразованием*, если F совпадает с G и σ'' — тождественный автоморфизм (т. е. $\sigma'' = 1$).

Из следующего классического примера видно, что понятие полулинейного преобразования является более общим, чем понятие линейного преобразования, даже тогда, когда мы ограничимся лишь одним F-пространством. Пусть F есть поле комплексных чисел, а A — плоскость над F, которая состоит из всех троек (c_1, c_2, c_3) комплексных чисел. Через $\bar{c}$ обозначим сопряженное с c комплексное число, а через σ — отображение плоскости A на себя, при котором образом тройки (c_1, c_2, c_3) является

$$(c_1, c_2, c_3)^\sigma = (\bar{c}_1, \bar{c}_2, \bar{c}_3).$$

Легко проверить, что пара, состоящая из σ и отображения $c \longrightarrow \bar{c}$, будет полулинейным преобразованием. Более подробное изучение «геометрических» различий между линейными и полулинейными преобразованиями будет дано ниже в § 2.

Предложение 2. *Полулинейные преобразования индуцируют проективные отображения.*

Доказательство. Если σ есть полулинейное преобразование F-пространства A на G-пространство B и если S — подпространство F-пространства A, то множество S^σ образов s^σ всех элементов s из S является подпространством G-пространства B. [Для проверки этого утверждения достаточно принять во внимание, что для каждого элемента g тела G существует такой однозначно определенный элемент f тела F, что $f^\sigma = g$; поэтому элемент $gs^\sigma = f^\sigma s^\sigma = (fs)^\sigma$ принадлежит S^σ, если s принадлежит S.] Следовательно, отображение подпространств S F-пространства A на подпространства S^σ G-пространства B является искомым «*индуцированным*» проективным отображением A на B.

Предложение 3. *Пусть ранг F-пространства A больше 1. Тогда*:

(а) *Если однозначное отображение σ F-пространства A в себя удовлетворяет условиям*

$$(a' + a'')^\sigma = a'^\sigma + a''^\sigma \text{ для } a', a'' \text{ из } A$$

и

$$S^\sigma \leqslant S$$

для каждого подпространства S F-пространства A, то или $A^\sigma = 0$ (т. е. $\sigma = 0$), или σ является полулинейным преобразованием.

(б) *Отображение σ F-пространства A в себя тогда и только тогда является полулинейным преобразованием, удовлетворяющим условию $S^\sigma \leqslant S$ для каждого подпространства S, когда в F существует такое отличное от нуля число f, что $a^\sigma = fa$ для каждого элемента a из A.*

Значение этого предложения состоит в том, что в нем описываются все преобразования линейного многообразия, индуцирующие тождественное проективное отображение.

Доказательство. Предположим сначала, что f — отличное от 0 число из F, и сопоставим каждому элементу a из A элемент $a^\sigma = fa$. Очевидно, что так определенное преобразование σ переводит сумму элементов в сумму соответствующих элементов и удовлетворяет условию $S^\sigma = S$ для каждого подпространства S F-пространства A. Если $a \in A$ и $x \in F$, то

$$(xa)^\sigma = f(xa) = (fxf^{-1})fa = x^\sigma a^\sigma,$$

где отображение $x^\sigma = fxf^{-1}$ является внутренним автоморфизмом тела F. Таким образом, σ представляет собой полулинейное преобразование, индуцирующее тождественное проективное отображение. (Заметим, что σ тогда и только тогда будет линейным преобразованием, когда элемент f перестановочен с каждым элементом тела F.)

Пусть теперь однозначное отображение σ F-пространства A в себя удовлетворяет условиям

$$(a' + a'')^\sigma = a'^\sigma + a''^\sigma \text{ для } a', a'' \text{ из } A$$

и

$$S^\sigma \leqslant S$$

для каждого подпространства S F-пространства A. Очевидно, что $0^\sigma = 0$. Если x — отличный от 0 элемент из A, то, в силу второго условия, $(Fx)^\sigma \leqslant Fx$. Таким образом, x^σ принадлежит Fx, и, следовательно, в F существует, и притом только одно, такое число f_x, что $x^\sigma = f_x x$.

Пусть x и y — линейно независимые элементы F-пространства A. Тогда ни один из элементов x, y, $x+y$ не равен 0; поэтому имеет место равенство

$$f_{x+y}x + f_{x+y}y = f_{x+y}(x+y) = (x+y)^\sigma = x^\sigma + y^\sigma = f_x x + f_y y,$$

из которого, в силу линейной независимости элементов x и y, следует, что

$$f_x = f_{x+y} = f_y.$$

Предположим теперь, что x и y — линейно зависимые отличные от 0 элементы F-пространства A. Тогда, поскольку $r(A) > 1$, существует элемент z, линейно не зависящий от обоих элементов x и y; поэтому, как следует из предыдущего, $f_x = f_y = f_z$.

Таким образом, мы показали, что равенство $f_x = f_y$ справедливо для любой пары отличных от 0 элементов x и y из A. Обозначив все равные друг другу числа f_x через f, мы получим, очевидно, что $a^\sigma = fa$ для каждого a из A. Если $f = 0$, то $\sigma = 0$; если $f \neq 0$, то, как было показано выше, σ является полулинейным преобразованием. Этим наше предложение полностью доказано.

Следствие 1. *Если $Fx = Fy$, то существует такое полулинейное преобразование σ F-пространства A на себя, при котором $x^\sigma = y$ и $S^\sigma = S$ для каждого подпространства S.*

Это утверждение при $r(A) = 1$ очевидно, а при $r(A) > 1$ почти непосредственно вытекает из предложения 3.

Следствие 2. *Если $r(A) > 1$, то полулинейные преобразования σ и τ F-пространства A на G-пространство B тогда и только тогда индуцируют одно и то же проективное отображение, когда в теле G существует такое число $g \neq 0$, что $a^\sigma = ga^\tau$ для каждого a из A.*

Доказательство. Полулинейные преобразования σ и τ тогда и только тогда индуцируют одно и то же проективное отображение, когда полулинейное преобразование $\sigma\tau^{-1}$ индуцирует тождественное проективное отображение. Последнее условие, в силу предложения 3, эквивалентно существованию такого числа $f \neq 0$ из F, что $a^{\sigma\tau^{-1}} = fa$ для каждого a из A. Но это равенство справедливо тогда и только тогда, когда

$$a^\sigma = (fa)^\tau = f^\tau a^\tau = ga^\tau$$

для каждого a из A, где $g = f^\tau$.

Читатель легко может убедиться в том, что предложение 3 и следствие 2 перестают быть справедливыми без предположения, что $r(A) > 1$.

ПЕРВАЯ ОСНОВНАЯ ТЕОРЕМА ПРОЕКТИВНОЙ ГЕОМЕТРИИ

Если ранг линейного многообразия (F, A) не меньше 3, то каждое проективное отображение F-пространства A индуцируется полулинейным преобразованием.

(Группу предложений, которую обычно называют «основной теоремой проективной геометрии», мы рассмотрим в § 3.)

Доказательство нашей теоремы будет разбито на несколько этапов. Пусть нам даны F-пространство A, G-пространство B и проективное отображение A на B, при котором подпространство S F-пространства A отображается на подпространство S^* G-пространства B. Предположим, кроме того, что $r(A) > 2$, хотя это

предположение мы используем лишь к концу нашего доказательства.

Из предложения 1 следует, что S и S^* имеют один и тот же ранг, так что, в частности, образ $(Fx)^*$ для $x \neq 0$ будет некоторой точкой Gy. Докажем следующие утверждения.

(1) *Если Fx и Fy — две различные точки F-пространства A и если x' — такой элемент G-пространства B, что $(Fx)^* = Gx'$, то в B существует, и притом только один, элемент $y' = h(x, x', y)$, удовлетворяющий условиям $(Fy)^* = Gy'$ и $[F(x-y)]^* = G(x'-y')$.*

Доказательство. Поскольку $F(x-y) \leqslant Fx + Fy$, мы имеем

$$[F(x-y)]^* \leqslant (Fx)^* + (Fy)^*.$$

Так как $F(x-y)$ и $[F(x-y)]^*$ являются точками, то $[F(x-y)]^* = Gt$, причем элемент t непременно содержится в подпространстве $(Fx)^* + (Fy)^*$. Отсюда и из равенства $(Fx)^* = Gx'$ следует существование такого числа $g \in G$ и такого элемента $z \in (Fy)^*$, что $t = gx' - z$. Предположим, что $g = 0$; тогда t принадлежит $(Fy)^*$ и потому $[F(x-y)]^* \leqslant (Fy)^*$. Но отсюда следует, что $F(x-y) \leqslant Fy$, так что элемент x содержится в Fy, и поэтому $Fx = Fy$, что невозможно. Точно так же можно доказать, что $z \neq 0$. Положим $y' = g^{-1}z$. Элемент y' отличен от 0, и, поскольку он содержится в $(Fy)^*$, $(Fy)^* = Gy'$. Кроме того,

$$[F(x-y)]^* = Gt = Gg^{-1}t = G(x'-y');$$

таким образом, элемент y' удовлетворяет всем нашим требованиям.

Пусть теперь в B существует еще один такой элемент y'', что $(Fy)^* = Gy''$ и $[F(x-y)]^* = G(x'-y'')$. Тогда

$$Gy' = Gy'' \text{ и } G(x'-y') = G(x'-y'').$$

Но это означает, что в G существуют такие отличные от 0 числа u, v, что $y' = uy''$ и

$$v(x'-y'') = x'-y' = x'-uy''.$$

Так как Gx' и Gy'' — различные точки, то элементы x' и y'' G-пространства B линейно независимы. Из этого замечания и из равенства $vx' - vy'' = x' - uy''$ следует, что $v = 1$ и $v = u$; отсюда $y' = y''$, что и требовалось доказать.

Однозначная функция $h(x, x', y)$ определена для каждой пары линейно независимых элементов x и y из A и произвольного элемента x' из B, удовлетворяющего условию $(Fx)^* = Gx'$. Очевидно, что она также зависит и от данного проективного отображения *. Целесообразно положить $h(x, x', 0) = 0$; это согласуется с предыдущим определением функции h, поскольку $0^* = \mathfrak{0} = G0$.

(2) *$h(x, x', y) = y'$ тогда и только тогда, когда $h(y, y', x) = x'$.*

Доказательство. Это утверждение непосредственно следует из однозначности функции h и из того, что элементы $y'=h(x, x', y)$ и $x'=h(y, y', x)$ определяются одной и той же системой уравнений, а именно

$$(Fx)^*=Gx',\ [F(x-y)]^*=G(x'-y'),\ (Fy)^*=Gy'.$$

(3) *Если x, y, z — линейно независимые элементы F-пространства A, то*

$$F(y-z)=[Fy+Fz]\cap[F(x-y)+F(x-z)].$$

Доказательство. Очевидно, что

$$F(y-z)\leqslant[Fy+Fz]\cap[F(x-y)+F(x-z)]=J.$$

Обратно, если j — некоторый элемент из J, то, поскольку j содержится в двух подпространствах $Fy+Fz$ и $F(x-y)+F(x-z)$, это можно представить в виде

$j=ay+bz=d(x-y)+e(x-z)$, где a, b, d, e — числа из F.

Так как элементы x, y, z линейно независимы, то из полученного равенства вытекает, что $a=-d$, $b=-e$, $0=d+e$. Отсюда $a=-b$, и, следовательно, $j=a(y-z)$ содержится в $F(y-z)$. Таким образом, $J=F(y-z)$, чем и завершается доказательство нашего утверждения.

(4) *Если x, y, z — линейно независимые элементы F-пространства A, то из равенств $h(x, x', y)=y'$ и $h(x, x', z)=z'$ следует, что $h(y, y', z)=z'$.*

Доказательство. Из наших предположений вытекает справедливость следующих равенств:

$$(Fx)^*=Gx',\ (Fy)^*=Gy',\ (Fz)^*=Gz',$$
$$[F(x-y)]^*=G(x'-y'),\ [F(x-z)]^*=G(x'-z').$$

Линейная независимость элементов x', y', z' вытекает из линейной независимости элементов x, y, z (см. лемму 1). Следовательно, применяя как к элементам x, y, z из A, так и к элементам x', y', z' из B утверждение (3), мы получаем, что

$$[F(y-z)]^*=([Fy+Fz]\cap[F(x-y)+F(x-z)])^*=$$
$$=[(Fy)^*+(Fz)^*]\cap[(F(x-y))^*+(F(x-z))^*]=$$
$$=[Gy'+Gz']\cap[G(x'-y')+G(x'-z')]=G(y'-z').$$

Но, по определению функции h [см. (1)], справедливость трех равенств

$$(Fy)^*=Gy',\ [F(y-z)]^*=G(y'-z'),\ (Fz)^*=Gz'$$

означает, что $h(y, y', z)=z'$; таким образом, утверждение (4) доказано.

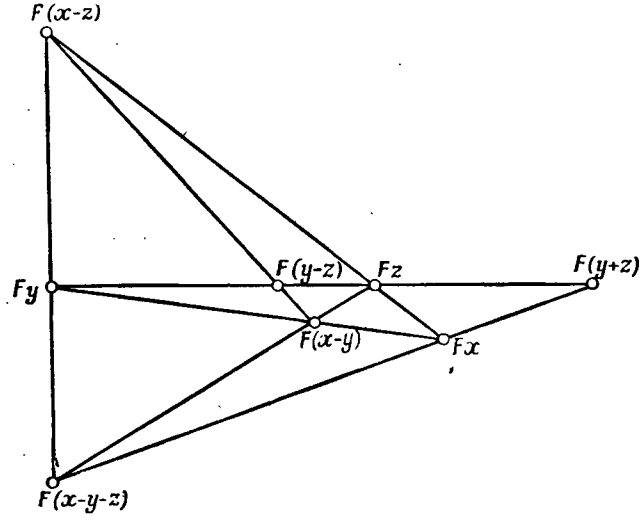
(5) *Если* x, y, z — *линейно независимые элементы* F-*пространства* A, *то*

$$F(x-y-z)=[F(x-y)+Fz]\cap[F(x-z)+Fy]$$

и

$$F(y+z)=[Fy+Fz]\cap[F(x-y-z)+Fx].$$

Проверку справедливости этого утверждения мы оставляем читателю, поскольку она совершенно аналогична доказательству



Фиг. 2.

утверждения (3) (см. фиг. 2). Убедиться в справедливости утверждения (5) можно и другим способом, а именно: легко проверить, что пересечения, стоящие в правых частях равенств, имеют ранги, не превышающие 1, u содержат соответствующие точки из левых частей равенств.

(6) *Пусть* Fx — *точка и* $(Fx)^*=Gx'$. *Тогда, если*

$$Fx\cap(Fy+Fz)=0,$$

то

$$h(x,\ x',\ y+z)=h(x,\ x',\ y)+h(x,\ x',\ z).$$

Доказательство. Рассмотрим два различных случая.

Случай 1: элементы x, y, z F-пространства A линейно независимы. Пусть $y'=h(x, x', y)$ и $z'=h(x, x', z)$; тогда справедливы следующие равенства:

$$(Fx)^*=Gx',\ (Fy)^*=Gy',\ (Fz)^*=Gz',$$

$$[F(x-y)]^*=G(x'-y'),\ [F(x-z)]^*=G(x'-z').$$

Из линейной независимости элементов x, y, z вытекает линейная независимость элементов x', y', z'. Поэтому обе тройки элементов x, y, z и x', y', z' удовлетворяют условию утверждения (5). Следовательно,

$$[F(x-y-z)]^* = ([F(x-y)+Fz] \cap [F(x-z)+Fy])^* =$$
$$= ([F(x-y)]^* + (Fz)^*) \cap ([F(x-z)]^* + (Fy)^*) =$$
$$= [G(x'-y')+Gz'] \cap [G(x'-z')+Gy'] = G(x'-y'-z');$$

используя это равенство, мы подобным же образом получаем, что

$$[F(y+z)]^* = ([Fy+Fz] \cap [F(x-y-z)+Fx])^* =$$
$$= [(Fy)^* + (Fz)^*] \cap [(F(x-y-z))^* + (Fx)^*] =$$
$$= [Gy'+Gz'] \cap [G(x'-y'-z')+Gx'] = G(y'+z').$$

Но, по определению функции h [см. (1)], равенства $(Fx)^* = Gx'$, $[F(x-y-z)]^* = G(x'-y'-z')$ и $[F(y+z)]^* = G(y'+z')$ означают, что $h(x, x', y+z) = y'+z'$. Таким образом, наше утверждение в первом случае доказано.

Случай 2: элементы x, y, z линейно зависимы. Если хотя бы один из элементов y, z равен 0, то справедливость утверждения очевидна, поскольку мы положили $h(x, x', 0) = 0$. Поэтому допустим, что y и z оба отличны от 0; тогда, в силу наших предположений, Fx и $Fy = Fz$ являются двумя различными точками. Но, в силу нашего основного предположения, ранг F-пространства A больше двух; поэтому в A существует такая точка Fw, что три точки Fx, $Fy = Fz$, Fw независимы.

В таком случае или $y+z=0$, или три элемента x, $y+z$, w линейно независимы. Поскольку $Fy = Fz$, очевидна линейная независимость элементов $x, w+y, z$; линейно независимы также и элементы x, w, y. Используя теперь несколько раз показанное выше (случай 1), а также то, что $h(x, x', y+z) = 0$, если $y+z=0$, мы получаем

$$h(x, x', w) + h(x, x', y+z) = h(x, x', w+y+z) = h(x, x', w+y) +$$
$$+ h(x, x', z) = h(x, x', w) + h(x, x', y) + h(x, x', z);$$

отсюда следует требуемое равенство

$$h(x, x', y+z) = h(x, x', y) + h(x, x', z).$$

Таким образом, утверждение (6) доказано.

Теперь мы сделали все необходимые приготовления для того, чтобы построить нужное нам полулинейное преобразование. Поскольку ранг F-пространства A не меньше трех, мы можем выбрать в A (и притом многими различными способами) три линейно независимых элемента u, v, w. Так как $(Fu)^*$ является точкой, то можно выбрать в B (и притом многими различными способами) такой

элемент u', что $(Fu)^* = Gu'$. Пусть $h(u, u', v) = v'$ и $h(u, u', w) = w'$; тогда из утверждений (2) и (4) следует, что

(7) *$h(x, x', y) = y'$, если x и y — любые два различных элемента из трех элементов u, v, w.*

Далее, $h(x, x', 0) = 0$ для $x = u, v, w$. Пусть теперь t — некоторый отличный от 0 элемент F-пространства A. Тогда Ft является точкой, отличной по крайней мере от двух из трех точек Fu, Fv, Fw.

(8) *Если Fx и Fy — две различные точки из числа точек Fu, Fv, Fw и если точка Ft отлична от Fx и Fy, то*

$$h(x, x', t) = h(y, y', t).$$

Доказательство. Предположим ради удобства, что $x = u$ и $y = v$. Если точка Ft не лежит на прямой $Fu + Fv$, то три элемента u, v, t линейно независимы. Пусть $h(u, u', t) = t'$. Тогда из $h(u, u', v) = v'$ и $h(u, u', t) = t'$ следует, в силу утверждения (4), что $h(v, v', t) = t'$, т. е. в этом случае наше утверждение справедливо. Если же точка Ft лежит на прямой $Fu + Fv$, то из наших предположений вытекает, что через Ft не проходит ни одна из прямых $Fu + Fw$ и $Fv + Fw$. Тогда точно так же, как и в предыдущем случае, лишь дополнительно используя утверждение (7), можно показать, что $h(u, u', t) = h(w, w', t) = h(v, v', t)$; этим утверждение (8) полностью доказано.

Таким образом, мы убедились, что для каждого элемента t из A определены по крайней мере два из трех функциональных значений $h(u, u', t)$, $h(v, v', t)$, $h(w, w', t)$ и что те из этих значений, которые определены, совпадают между собой; их общее значение мы обозначим через t^σ. Другими словами:

(9) *Если x — один из трех элементов u, v, w, то $h(x, x', t)$ или не определено, или принимает однозначное*[1]) *значение t^σ.*

Таким образом, мы построили однозначное отображение σ элементов F-пространства A на элементы F-пространства B. Это отображение обладает следующими свойствами.

(10) *$(Ft)^* = Gt^\sigma$ для каждого t из A.*

Свойство (10) непосредственно следует из определения функции h [см. (1)].

(11) *$(a + b)^\sigma = a^\sigma + b^\sigma$ для a, b из A.*

Доказательство. Так как элементы u, v, w линейно независимы, то по крайней мере одна из точек Fu, Fv, Fw не лежит на прямой $Fa + Fb$. Если, например, Fu не лежит на $Fa + Fb$, то из определения отображения σ и из утверждения (6) следует, что

$$(a + b)^\sigma = h(u, u', a + b) = h(u, u', a) + h(u, u', b) = a^\sigma + b^\sigma,$$

как мы и утверждали.

[1]) То есть не зависящее от выбора x. — *Прим. перев.*

(12) *σ является изоморфным отображением аддитивной группы A на аддитивную группу B.*

Доказательство. Если $t^\sigma = 0$, то, в силу (10), $0 = Gt^\sigma = (Ft)^*$ и, следовательно, $t = 0$. Таким образом, σ является изоморфным отображением A в B [из $a^\sigma = b^\sigma$ следовало бы $(a-b)^\sigma = 0$, и т. д.]. Пусть теперь s — произвольный элемент из B. Так как $0^\sigma = 0$, то мы можем предположить, что $s \neq 0$. Тогда Gs будет точкой G-пространства B, а поэтому, как следует из свойств проективных отображений [см. (г)], существует такая единственная точка T F-пространства A, для которой $T^* = Gs$. Точка T отлична по крайней мере от одной из точек Fu, Fv, Fw. Поэтому без ущерба для общности доказательства можно предположить, что $T \neq Fu$. Тогда $Gs \neq Gu'$. Рассмотрим точку $G(u' + s)$, лежащую на прямой

$$Gu' + Gs = (Fu)^* + T^* = [Fu + T]^*.$$

По той же причине, что и в предыдущем случае, существует, и притом единственная, точка P, лежащая на прямой $Fu + T$, для которой $P^* = G(u' + s)$. Так как $T^* = Gs \neq G(u' + s) = P^*$, то $T \neq P$; теперь легко усмотреть, что точка P прямой $Fu + T$ имеет вид $P = F(u + t)$, где t принадлежит T (т. е. $T = Ft$). Отсюда, используя утверждения (10) и (11), мы получаем

$$G(u' + s) = P^* = [F(u + t)]^* = G(u + t)^\sigma = G(u^\sigma + t^\sigma) = G(u' + t^\sigma).$$

Таким образом, элемент $s - t^\sigma$ принадлежит пересечению подпространств P^* и $Gs = T^* = (Ft)^* = Gt^\sigma$, которое равно 0, поскольку P^* и T^* — различные точки. Следовательно, $s = t^\sigma$, и тем самым показано, что $A^\sigma = B$.

(13) *$S^* = S^\sigma$ для каждого подпространства S F-пространства A.*

Это утверждение легко следует из (10) и (12).

Если t — отличный от 0 элемент F-пространства A и f — отличное от 0 число из F, то, в силу (10), $Gt^\sigma = (Ft)^* = [F(ft)] = G(ft)^\sigma$; поэтому в G существует единственное число $g(f, t) \neq 0$, такое, что $(ft)^\sigma = g(f, t)\, t^\sigma$. Если положить $g(0, t) = 0$, то равенство

$$(ft)^\sigma = g(f, t)\, t^\sigma$$

будет справедливо для каждого f из F и каждого $t \neq 0$ из A.

(14) *$g(f, x) = g(f, y)$ для каждого числа f из F и любых отличных от 0 элементов x и y из A.*

Доказательство. Пусть сначала Fx и Fy являются различными точками. Тогда, как легко проверить, имеет место

равенство

$$g(f, x+y)\,x^\sigma + g(f, x+y)\,y^\sigma = g(f, x+y)\,(x+y)^\sigma = [f(x+y)]^\sigma =$$
$$= [fx+fy]^\sigma = (fx)^\sigma + (fy)^\sigma = g(f, x)\,x^\sigma + g(f, y)\,y^\sigma.$$

Так как Fx и Fy — различные точки, то также различными будут точки $Gx^\sigma = (Fx)^*$ и $Gy^\sigma = (Fy)^*$. Отсюда следует, что элементы x^σ и y^σ линейно независимы. Поэтому

$$g(f, x) = g(f, x+y) = g(f, y).$$

Если точки Fx и Fy совпадают, то существует точка $Fz \neq Fx = Fy$. Из показанного в предыдущем случае следует, что $g(f, x) = g(f, z) = g(f, y)$. Таким образом, утверждение (14) доказано.

Совпадающие между собой значения $g(f, x)$ для всех $x \neq 0$ из A мы обозначим через f^σ. Таким образом, σ индуцирует такое однозначное отображение тела F в тело G, обозначаемое нами также через σ, что

(15) $(ft)^\sigma = f^\sigma t^\sigma$ *для* f *из* F *и* t *из* A.

Покажем теперь, что

(16) σ *является изоморфным отображением тела* F *на тело* G.

Доказательство. Если x и y — элементы тела F и если t — некоторый отличный от 0 элемент F-пространства A, то, используя утверждение (15), мы получаем

$$(x+y)^\sigma t^\sigma = [(x+y)\,t]^\sigma = [xt+yt]^\sigma = (xt)^\sigma + (yt)^\sigma =$$
$$= x^\sigma t^\sigma + y^\sigma t^\sigma = (x^\sigma + y^\sigma)\,t^\sigma;$$

отсюда, поскольку $t^\sigma \neq 0$, следует, что $(x+y)^\sigma = x^\sigma + y^\sigma$.

Точно так же мы убеждаемся в справедливости равенства

$$(xy)^\sigma t^\sigma = [(xy)\,t]^\sigma = [x\,(yt)]^\sigma = x^\sigma\,(yt)^\sigma = x^\sigma\,(y^\sigma t^\sigma) = (x^\sigma y^\sigma)\,t^\sigma,$$

из которого следует, что $(xy)^\sigma = x^\sigma y^\sigma$; после этого становится очевидным, что σ является изоморфным отображением тела F в тело G. Если, наконец, z — произвольный элемент из G и t — отличный от 0 элемент F-пространства A, то, в силу утверждения (12), в A существует такой элемент s, для которого $s^\sigma = zt^\sigma$. Поэтому, ввиду (10),

$$(Fs)^* = Gs^\sigma = Gzt^\sigma = Gt^\sigma = (Ft)^*,$$

откуда $Fs = Ft$. Следовательно, в F существует такой элемент k, что $s = kt$; теперь из утверждения (15) вытекает, что $zt^\sigma = s^\sigma = (kt)^\sigma = k^\sigma t^\sigma$, и, так как $t^\sigma \neq 0$, то $z = k^\sigma$. Таким образом, $F^\sigma = G$, и этим утверждение (16) доказано.

Из утверждений (12), (15) и (16) вытекает, что σ является полулинейным преобразованием F-пространства A на G-простран-

ство B, а в силу утверждения (13), это полулинейное преобразование индуцирует заданное проективное отображение. Таким образом, наша теорема полностью доказана.

Замечание 1. Следующие соображения показывают необходимость сделанного в формулировке теоремы предположения, что $r(A) > 2$. Если F-пространство A является прямой [т. е. $r(A) = 2$], то его подпространствами, кроме 0 и A, будут только точки; различные же точки не могут содержаться одна в другой. Поэтому каждое взаимно однозначное отображение множества всех точек F-пространства A на множество всех точек G-пространства B, ранг которого равен 2, можно дополнить отображениями 0 на 0 и A на B до проективного отображения прямой A на прямую B. Ясно, что не все такие проективные отображения прямой индуцируются полулинейными преобразованиями. Это можно иллюстрировать следующим примером. Пусть A является прямой над полем действительных чисел, а B — прямой над полем комплексных чисел. Обе эти прямые содержат континуальное множество точек, и, следовательно, к ним можно применить указанную выше конструкцию. С другой стороны, так как поля действительных и комплексных чисел не изоморфны, то не существует ни одного полулинейного преобразования прямой A на прямую B. Приведем еще один пример. Пусть L — прямая над полем рациональных чисел. Эта прямая содержит счетное множество точек. Следовательно, существует континуум перестановок[1]) точек прямой L, и поэтому L обладает континуумом автопроективных отображений. С другой стороны, каждое полулинейное преобразование прямой L на себя является линейным, а множество всех линейных преобразований этой прямой всего лишь счетно. Следовательно, существуют автопроективные отображения прямой L, которые не индуцируются полулинейными преобразованиями. Подобных примеров прямых, содержащих как конечное, так и бесконечное множество точек, можно построить очень много.

Замечание 2. В следующем параграфе будут установлены необходимые и достаточные условия, при которых проективное отображение индуцируется линейным преобразованием. Здесь же мы хотим только подчеркнуть, что проективно эквивалентные линейные многообразия могут быть определены над различными, хотя и изоморфными, телами, и в этом случае нельзя отобразить одно из них на другое с помощью линейного преобразования. Кроме того, читателю следует вспомнить приведенный нами ранее пример полулинейного преобразования плоскости над полем комплексных чисел, которое не являлось линейным. Это полулинейное преобразование индуцирует проективное отображение, которое,

[1]) Под перестановкой автор понимает взаимно однозначное отображение какого-либо множества на себя. См. добавление М.—*Прим. перев.*

как легко проверить, не может быть индуцировано никаким линейным преобразованием.

Заметим, что выражение «проективно эквивалентные линейные многообразия» означает, что существует проективное отображение одного из этих линейных многообразий на другое.

Структурная теорема проективной геометрии. *F-пространство A и G-пространство B проективно эквивалентны тогда и только тогда, когда выполняются следующие условия:*

(а) $r(A) = r(B)$;

(б) $r(A) = r(B) = 1$; *или* $r(A) = r(B) = 2$, *и тела F и G содержат одно и то же число элементов*; *или* $r(A) = r(B) > 2$, *и тела F и G изоморфны.*

Доказательство. Необходимость условия (а) следует из предложения 1, в силу которого проективно эквивалентные линейные многообразия имеют равные ранги.

Очевидно, что две любые точки проективно эквивалентны. Если F-пространство A является прямой [т. е. $r(A) = 2$], то A обладает базисом, состоящим из двух элементов u, v, и каждую точку прямой A, отличную от Fv, можно однозначно представить в виде $F(u + xv)$, где $x \in F$. Таким образом, если d — число элементов тела F, то число точек, принадлежащих прямой A, равно $d+1$. Поэтому прямые A и B тогда и только тогда содержат одно и то же число точек, когда тела F и G состоят из одного и того же числа элементов. Отсюда и из замечания 1 следует, что прямые проективно эквивалентны тогда и только тогда, когда соответствующие им тела состоят из одного и того же числа элементов.

Если, наконец, F-пространство A и G-пространство B имеют один и тот же ранг, больший 2, то каждое проективное отображение A на B индуцируется некоторым полулинейным преобразованием. Таким образом, из проективной эквивалентности F-пространства A и G-пространства B следует изоморфность тел F и G. Обратно, если тела F и G изоморфны, то выберем некоторый базис A_0 линейного многообразия (F, A) и некоторый базис B_0 линейного многообразия (G, B). Так как $r(A) = r(B)$, то существует взаимно однозначное отображение τ множества A_0 на множество B_0; изоморфность же тел F и G означает, что существует определенное изоморфное отображение σ тела F на тело G. Отображая теперь «общий» элемент $\sum_{a \in A_0} f(a)\, a$ из A на элемент $\sum_{a \in A_0} f(a)^{\sigma} a^{\tau}$ из B, мы получаем полулинейное преобразование F-пространства A на G-пространство B, которое, как следует из предложения 2, индуцирует некоторое проективное отображение A на B. Таким образом, теорема полностью доказана.

Группа автопроективных отображений линейного многообразия (F, A), ранг которого не меньше 3, теперь

может быть представлена следующим образом. Обозначим через Π группу автопроективных отображений F-пространства A, а через Λ — группу полулинейных преобразований этого пространства на себя. Если σ принадлежит Λ, то, в силу предложения 2, σ индуцирует автопроективное отображение σ^* F-пространства A. Отображение σ в σ^* является, очевидно, гомоморфным [т. е. $(\sigma\tau)^* = \sigma^*\tau^*$], и, как вытекает из первой основной теоремы, группа Λ отображается при этом на всю группу $\Pi = \Lambda^*$. Из предложения 3 следует, что на единичный элемент группы Π отображаются лишь полулинейные преобразования σ из Λ вида $a^\sigma = fa$ для каждого a из A; такие полулинейные преобразования образуют нормальный делитель N группы Λ. Таким образом, группа Π по существу тождественна фактор-группе Λ/N.

Историческая справка. Первое удовлетворительное доказательство теоремы типа нашей первой основной теоремы проективной геометрии принадлежит Е. Камке.

Добавление I

Проективная конструкция группы гомотетий

Линейное многообразие (F, A) определяет проективную геометрию, образованную подпространствами F-пространства A. Но, согласно первой основной теореме проективной геометрии (§ 1), строение этой проективной геометрии полностью определяет алгебраическое строение линейного многообразия. Поэтому должно быть возможным восстановление линейного многообразия $(F, A$ по проективной геометрии его подпространств. Эту проблему можно рассматривать в двух существенно различных аспектах. При самой общей постановке указанной проблемы предполагается, что дана абстрактная проективная геометрия [1]), о которой заранее не известно, что элементами ее являются подпространства некоторого линейного многообразия, и основная задача состоит в том, чтобы найти то линейное многообразие, проективная геометрия подпространств которого проективно эквивалентна данной проективной геометрии. Другая, более легкая, постановка той же проблемы состоит в том, что нам заранее известно, что данная проективная геометрия образована подпространствами некоторого линейного многообразия, и мы хотим доказать, что это линейное многообразие по существу тождественно с некоторым линейным многообразием, строящимся на основе данной проективной геометрии. Решению первой из указанных проблем мы посвятим гл. VII; настоящее же добавление касается лишь последней проблемы.

[1]) Аксиомы абстрактной проективной геометрии изложены в гл. VII, §§ 1 и 3. — *Прим. перев.*

Тем не менее многие построения и рассуждения, приводимые здесь, аналогичны тем методам, которыми мы воспользуемся в гл. VII (и поэтому могут служить подготовкой к ним).

В настоящем добавлении мы будем строить не столько само линейное многообразие, сколько некоторую группу преобразований, тесно связанную с этим линейным многообразием.

Если f — отличный от 0 элемент тела F и w — некоторый элемент F-пространства A, то преобразование σ, определяемое равенством

$$x^\sigma = fx + w \text{ для каждого } x \text{ из } A,$$

называется *гомотетией* линейного многообразия (F, A). Очевидно, что совокупность всех гомотетий данного F-пространства A является группой, а именно *группой гомотетий* H линейного многообразия (F, A). Эта группа содержит две особенно интересные для нас подгруппы: группу T всех *движений*, т. е. преобразований σ вида $x^\sigma = x + w$, и группу Δ всех *растяжений*, состоящую из преобразований σ вида $x^\sigma = fx$. Сопоставляя элементу w из A движение $x^\sigma = x + w$, мы получаем (естественный) изоморфизм аддитивной группы A на мультипликативную группу движений; аналогично, отображение каждого элемента $f \neq 0$ из F на растяжение $x^\sigma = f^{-1}x$ является (естественным) изоморфизмом мультипликативной группы тела F на мультипликативную группу растяжений. (Читатель может самостоятельно убедиться в справедливости этих простых утверждений.)

Очевидно, что каждую гомотетию η линейного многообразия (F, A) можно однозначно представить в виде $\eta = \delta\tau$, где δ — растяжение и τ — движение. Пусть теперь β является движением, т. е. $x^\beta = x + b$, и σ — гомотетией, т. е. $x^\sigma = fx + w$. Тогда прямым подсчетом легко проверить, что

$$x^{\sigma^{-1}\beta\sigma} = x + fb \text{ для каждого } x \text{ из } A.$$

Таким образом, группа движений T является нормальным делителем группы гомотетий H. При этом внутренние автоморфизмы группы H индуцируют подгруппу группы автоморфизмов группы T, изоморфную группе растяжений Δ и мультипликативной группе тела F.

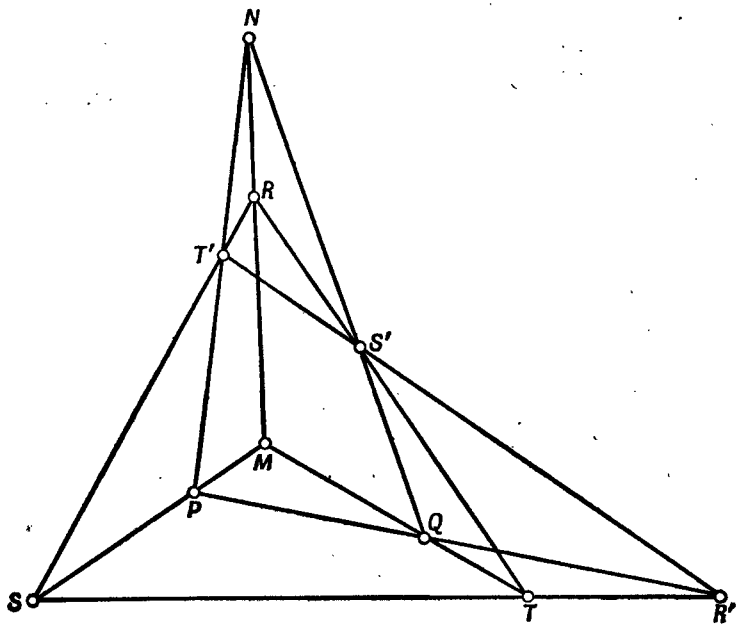
Из предыдущего замечания становится очевидным, что строение линейного многообразия (F, A) полностью определяется строением расширения H группы T при помощи группы Δ; этим оправдывается наша цель дать проективную конструкцию группы гомотетий и ее подгрупп движений и растяжений.

Элементами наших групп будут специальные преобразования некоторых объектов, причем и те и другие мы определим в понятиях исходной проективной геометрии. Естественно, что прежде всего нужно определить объекты преобразований. Это будет сделано в два этапа.

Основной шестеркой называется *упорядоченное* множество, состоящее из шести точек R, S, T; R', S', T' линейного многообразия (F, A), удовлетворяющее следующим условиям:

$$\left.\begin{array}{l}\text{Точки } R, S, T \text{ независимы (т. е. порождают плоскость).}\\ \text{Если } X, Y, Z \text{ есть любая перестановка букв } R, S, T, \text{ то}\\ \qquad X+Y=Y+Z'=Z'+X.\\ \qquad R'+S'=S'+T'=T'+R'.\end{array}\right\} \quad (\text{I. 1})$$

Очевидно, что три точки R', S', T' определяют одну прямую L и что эта прямая пересекает стороны треугольника R, S, T как раз в точках T', R', S'.



Фиг. 3.

Основная шестерка может существовать лишь тогда, когда ранг линейного многообразия (F, A) не меньше 3. Поэтому всюду в этом добавлении предполагается, что $r(A) > 2$.

Предложение 1. (а) *Если r, s, t — три линейно независимых элемента F-пространства A, то точки Fr, Fs, Ft; $F(s-t)$, $F(t-r)$, $F(r-s)$ образуют основную шестерку, которую мы будем называть основной шестеркой, определяемой тройкой r, s, t линейно независимых элементов.*

(б) *Каждая основная шестерка определяется некоторой тройкой линейно независимых элементов.*

(в) *Тройки* r, s, t *и* u, v, w *линейно независимых элементов тогда и только тогда определяют одну и ту же основную шестерку, когда в теле* F *существует такое число* $f \neq 0$, *что* $u = fr$, $v = fs$, $w = ft$.

Доказательство. Утверждения (а) и (в) проверяются достаточно просто, так что мы предоставляем это сделать читателю. Чтобы доказать утверждение (б), рассмотрим произвольную основную шестерку $R, S, T; R', S', T'$ и выберем любой такой элемент r F-пространства A, что $R = Fr$. Так как точка R лежит на прямой $S + T'$, то существуют такие элементы s и t', содержащиеся соответственно в S и T', что $r = s + t'$. Поскольку три точки R, S, T' попарно различны, каждый из элементов s и t' отличен от 0. Поэтому $S = Fs$ и $T' = Ft' = F(r - s)$. Аналогично доказывается существование такого элемента t, что $T = Ft$ и $S' = F(t - r)$. Далее, так как точки R, S, T порождают плоскость, то элементы r, s, t линейно независимы. Поэтому точка R', через которую проходят прямые $S + T$ и $S' + T'$, является единственной точкой пересечения этих прямых, т. е.

$$R' = (S + T) \cap (S' + T') = (Fs + Ft) \cap (F[t - r] + F[r - s]).$$

Но, как легко проверить, это пересечение содержит точку $F(s - t)$. Отсюда следует, что $R' = F(s - t)$. Таким образом, данная основная шестерка определяется тройкой r, s, t линейно независимых элементов, что и требовалось доказать.

Допустимой четверкой (относительно данной основной шестерки $R, S, T; R', S', T'$) называется *упорядоченное* множество $[M, N, P, Q]$ подпространств линейного многообразия (F, A), удовлетворяющих следующим условиям:

$$\left.\begin{array}{c} r(X) \leqslant 1 \quad \text{для} \quad X = M,\ N,\ P,\ Q, \\ M + R = R + N = N + M,\ P + R' = R' + Q = Q + P, \\ M + S = S + P = P + M,\ Q + S' = S' + N = N + Q, \\ M + T = T + Q = Q + M,\ N + T' = T' + P = P + N. \end{array}\right\} \quad (\text{I. 2})$$

Легко видеть, что самое большее одна «координата» допустимой четверки может равняться 0 и что лишь следующие допустимые четверки имеют одну нулевую координату:

$$[0, R, S, T],\ [R, 0, T', S'],\ [S, T', 0, R'],\ [T, S', R', 0].$$

Предложение 2. *Если основная шестерка* $R, S, T; R', S', T'$ *определяется тройкой* r, s, t *линейно независимых элементов* F*-пространства* A, *то, сопоставляя каждому элементу* x *из* A *четверку*

$$[Fx,\ F(x - r),\ F(x - s),\ F(x - t)] = x^*,$$

мы получаем взаимно однозначное отображение F-пространства A на совокупность всех допустимых четверок.

Доказательство. Используя линейную независимость элементов r, s, t, легко проверить, что x^* для каждого x из A будет допустимой четверкой относительно основной шестерки Fr, Fs, Ft; $F(s-t)$, $F(t-r)$, $F(r-s)$. Если $x^*=y^*=[M, N, P, Q]$, то из определения отображения * следует, что $x-y$ содержится в пересечении $M\cap N\cap P\cap Q$, ибо, например, $x-y=(x-r)-(y-r)$. Но поскольку ранг каждого из подпространств M, N, P, Q не превышает 1, $M\cap N\cap P\cap Q=0$, так как в противном случае имело бы место равенство $M=N=P=Q$ и эта точка совпадала бы с точками R, S и T, что, очевидно, невозможно. Следовательно, $x-y=0$. Тем самым показано, что $x^*=y^*$ тогда и только тогда, когда $x=y$; таким образом, наше отображение является взаимно однозначным отображением F-пространства A в совокупность допустимых четверок.

Рассмотрим теперь произвольную допустимую четверку $J=[M, N, P, Q]$. Если одна из ее координат равняется 0, то, как было отмечено выше, J равняется или 0^*, или r^*, или s^*, или t^*. Поэтому можно предположить, что ни одна из координат допустимой четверки J не равняется 0. Рассмотрим отдельно два возможных случая.

Случай 1: точка M совпадает с одной из точек R, S, T. Без ограничения общности можно предположить, что $M=R=Fr$. Тогда, как следует из условия (I.2), N содержится в подпространстве $M+R=Fr$. Но поскольку N сама является точкой, мы получаем, что $M=N=R=Fr$. Далее, из равенства $M=Fr$ и условия (I.2) следует равенство $Fr+Fs=Fs+P=P+Fr$, в силу которого, в частности, существуют такой элемент p из P и такое число u из F, что $s=ur+p$, причем и u и p отличны от 0. Поэтому $P=Fp=F(ur-s)$; точно так же можно доказать существование в F такого числа $v\neq 0$, что $Q=F(vr-t)$. Теперь, вновь используя условие (I.2), мы получаем, что

$$F(s-t)=R'\leqslant P+Q=F(ur-s)+F(vr-t);$$

из этого включения и из линейной независимости элементов r, s, t следует, что $u=v$. Если бы u равнялось 1. то, ввиду (I.2), мы имели бы

$$Fr=N\leqslant P+T'=F(r-s),$$

что, в силу линейной независимости элементов r и s, невозможно; поэтому, как легко проверить, $J=(ur)^*$.

Случай 2: точка M отлична от каждой из трех точек R, S, T. Так как три прямые $R+S$, $S+T$, $T+R$ попарно различны, то точка M может лежать самое большее на одной из этих прямых;

поэтому можно предположить, что M не лежит на прямых $Fr+Fs$ и $Fs+Ft$.

Так как $R+M=M+N=N+R$ является прямой, то R, M, N — три попарно различные коллинеарные точки. Поэтому существуют такие однозначно определенные и отличные от 0 элементы m и n, содержащиеся соответственно в M и N, что $r=m+n$. Следовательно,

$$M=Fm \text{ и } N=Fn=F(r-m).$$

Если бы прямые

$$F(m-s)+Fs=Fm+Fs=M+S=S+P=P+M,$$

$$F(m-s)+F(s-r)=F(s-r)+F(m-r)=T'+N=N+P=P+T'$$

совпадали, то они совпадали бы с прямой $R+S$, а тем самым на прямой $R+S$ лежала бы точка M, что по нашим предположениям невозможно. Поэтому указанные две прямые имеют единственную точку пересечения; как легко видеть, этой точкой является точка $F(m-s)=P$. Аналогично можно показать, что $F(m-t)=Q$. Таким образом, $J=m^*$. Этим предложение 2 полностью доказано.

Замечание 1. Если основная шестерка R, S, T; R', S', T' определяется тройкой r, s, t линейно независимых элементов F-пространства A, то, как показывает предыдущее предложение, отображение элемента x из A на четверку

$$x^*=[Fx,\ F(x-r),\ F(x-s),\ F(x-t)]$$

является взаимно однозначным отображением F-пространства A на совокупность допустимых четверок. Если r^0, s^0, t^0 – другая тройка линейно независимых элементов из A, определяющая ту же самую основную шестерку, то мы получим другое взаимно однозначное отображение F-пространства A на совокупность допустимых четверок, при котором элемент x из A отображается на допустимую четверку

$$x^0=[Fx,\ F(x-r^0),\ F(x-s^0),\ F(x-t^0)].$$

В силу предложения 1 (в), в теле F существует такое число $g\neq 0$, что $u^0=gu$ для $u=r$, s, t. Используя это, легко проверить, что

$$(gx)^0=x^* \text{ для каждого } x \text{ из } A.$$

Таким образом, мы видим, что различным тройкам линейно независимых элементов, определяющим одну и ту же основную шестерку, соответствуют различные отображения F-пространства A на совокупность допустимых четверок; однако любые два таких отображения отличаются друг от друга лишь «тривиальным» полулинейным преобразованием вида $x^\sigma=gx$.

Читателю в качестве полезного упражнения предлагаем выразить координаты допустимой четверки $(x+y)^*$ через координаты допустимых четверок x^* и y^*. Мы, однако, этим результатом пользоваться не будем.

Фиксируем теперь некоторую основную шестерку R, S, T; R', S', T', которую обозначим через B. Совокупность всех допустимых относительно B четверок обозначим через $V(B)$. Координаты допустимых четверок будем обозначать следующим образом:

$$J=[J_O,\ J_R,\ J_S,\ J_T] \text{ для каждого } J \text{ из } V(B).$$

Гомотетией совокупности $V(B)$ мы называем такую перестановку σ элементов совокупности $V(B)$, для которой выполняется условие

$$(J_O+K_O)\cap(J_R+K_R)\cap(J_S+K_S)\cap(J_T+K_T)=$$
$$=(J_O^\sigma+K_O^\sigma)\cap(J_R^\sigma+K_R^\sigma)\cap(J_S^\sigma+K_S^\sigma)\cap(J_T^\sigma+K_T^\sigma) \quad (\Gamma)$$

при любых J и K из $V(B)$.

Гомотетия σ совокупности $V(B)$, удовлетворяющая условию

$$(J_O+J_O^\sigma)\cap(J_R+J_R^\sigma)\cap(J_S+J_S^\sigma)\cap(J_T+J_T^\sigma)=$$
$$=(K_O+K_O^\sigma)\cap(K_R+K_R^\sigma)\cap(K_S+K_S^\sigma)\cap(K_T+K_T^\sigma) \quad (Д)$$

для любых J и K из $V(B)$, называется *движением в* $V(B)$.

Гомотетия σ совокупности $V(B)$, удовлетворяющая условию

$$J_O^\sigma=J_O \text{ для каждого } J \text{ из } V(B), \quad (Р)$$

называется *растяжением в* $V(B)$.

Очевидно, что совокупность всех гомотетий является группой и что все растяжения образуют подгруппу этой группы. Труднее показать, что совокупность всех движений является нормальным делителем группы гомотетий; в справедливости этого утверждения мы убедимся в процессе последующих рассмотрений.

Пусть теперь r, s, t — некоторая тройка линейно независимых элементов F-пространства A, определяющая данную основную шестерку B. Тогда, отображая элемент x из A на допустимую четверку

$$x^*=[Fx,\ F(x-r),\ F(x-s),\ F(x-t)],$$

мы получаем взаимно однозначное отображение F-пространства A на совокупность $V(B)$. Если σ — некоторая перестановка элементов F-пространства A, то существует одна и только одна такая перестановка σ^* допустимых четверок из $V(B)$, что

$$(x^\sigma)^*=x^{*\sigma^*} \text{ для каждого } x \text{ из } A;$$

соответствие между σ и σ^* является изоморфизмом группы всех перестановок линейного многообразия (F, A) на группу всех перестановок совокупности $V(B)$.

Предложение 3. *При отображении $\sigma \to \sigma^*$ группа гомотетий, группа движений и группа растяжений линейного многообразия (F, A) изоморфно отображаются соответственно на группу гомотетий, совокупность движений и группу растяжений совокупности $V(B)$.*

Так как при изоморфном отображении нормальный делитель переходит в нормальный делитель, то из этого предложения следует, что движения в $V(B)$ образуют нормальный делитель группы гомотетий совокупности $V(B)$.

Доказательству этого предложения мы предпошлем доказательство следующего утверждения.

Лемма. *Если x и y — элементы F-пространства A, то*

$$F(x-y) = (x_O^* + y_O^*) \cap (x_R^* + y_R^*) \cap (x_S^* + y_S^*) \cap (x_T^* + y_T^*).$$

Доказательство. Правая часть доказываемого равенства представляет собой пересечение подпространств F-пространства A, которое мы обозначим через D, т. е.

$$D = (Fx + Fy) \cap [F(x-r) + F(y-r)] \cap \dots .$$

Очевидно, что $F(x-y)$ содержится в D. Так как три элемента r, s, t линейно независимы, то все они не могут одновременно принадлежать подпространству $Fx + Fy$; поэтому без ограничения общности можно предположить, что r не содержится в $Fx + Fy$. Каждый элемент d из D имеет вид

$$d = x'x + y'y = x''(x-r) + y''(y-r),$$

где x', y', x'', y'' — числа из F. Отсюда следует, что

$$(x''-x')x + (y''-y')y = (x''+y'')r.$$

Но поскольку r не содержится в $Fx + Fy$, предыдущее равенство возможно только в случае, когда $x''+y''=0$. Таким образом, $d = x''(x-y)$ и, следовательно, принадлежит $F(x-y)$, т. е. $D = F(x-y)$, что и требовалось доказать. [То, что $F(x-y)$ не является собственной частью подпространства D, можно было бы также доказать путем подсчета ранга $r(D)$.]

Из этой леммы непосредственно вытекает справедливость следующего утверждения.

Следствие. *Если σ есть перестановка F-пространства A и σ^* — соответствующая ей перестановка в $V(B)$, то*

(а) *σ^* тогда и только тогда обладает свойством* (Г), *когда $F(x-y) = F(x^\sigma - y^\sigma)$ для любых x и y из A;*

(б) *σ^* тогда и только тогда обладает свойством* (Д), *когда $F(x-x^\sigma) = F(y-y^\sigma)$ для любых x и y из A;*

(в) σ^* *тогда и только тогда обладает свойством* (Р), *когда* $Fx = Fx^\sigma$ *для каждого* x *из* A.

Если σ есть движение в A, то $x^\sigma = x + b$ для каждого x из A; следовательно, $x - y = x^\sigma - y^\sigma$ и $x - x^\sigma = -b = y - y^\sigma$. Поэтому σ^* является движением в $V(B)$. Если σ — растяжение в A, то $x^\sigma = fx$, где f — отличное от 0 фиксированное число из F, так что $x^\sigma - y^\sigma = f(x - y)$. Отсюда видно, что если σ является растяжением в A, то σ^* будет растяжением в $V(B)$. Подобным же образом можно показать, что если σ — гомотетия линейного многообразия (F, A), то σ^* — гомотетия совокупности $V(B)$. [Этот же результат можно также получить из предыдущих утверждений, принимая во внимание, что каждая гомотетия линейного многообразия (F, A) представима в виде произведения растяжения на движение.]

(1) *Гомотетия* η *совокупности* $V(B)$ *тогда и только тогда является растяжением, когда* $0^{*\eta} = 0^*$.

Доказательство. Если η — растяжение, то $0^{*\eta} = [0, \ldots]$. Но так как существует лишь одна допустимая четверка, первая координата которой равна 0, а именно 0^*, то $0^{*\eta} = 0^*$. Обратно, пусть при гомотетии η совокупности $V(B)$ будет $0^{*\eta} = 0^*$. В силу предыдущих результатов, существует одна и только одна перестановка σ F-пространства A, для которой $\sigma^* = \eta$. Очевидно, что $0^\sigma = 0$. Так как η удовлетворяет условию (Г), то, ввиду следствия (а), $Fx = F(x - 0) = F(x^\sigma - 0^\sigma) = Fx^\sigma$; отсюда и из следствия (в) вытекает, что $\sigma^* = \eta$ является растяжением, что и требовалось доказать.

(2) *Если* τ' *и* τ'' *являются такими движениями в* $V(B)$, *что* $0^{*\tau'} = 0^{*\tau''}$, *то* $\tau' = \tau''$.

Доказательство. Существуют такие перестановки σ' и σ'' F-пространства A, для которых $\sigma'^* = \tau'$ и $\sigma''^* = \tau''$. Поскольку $(x)^* = x^*$, из нашего предположения следует, что $0^{\sigma'} = 0^{\sigma''} = w$. Применяя теперь следствия (а) и (б) к случаю, когда $y = 0$, мы получаем

$$\left.\begin{aligned} F(x^{\sigma'} - w) &= Fx = F(x^{\sigma''} - w) \text{ для каждого } x \text{ из } A, \\ F(x^{\sigma'} - x) &= Fw = F(x^{\sigma''} - x) \text{ для каждого } x \text{ из } A. \end{aligned}\right\} \quad (2^*)$$

Если $w = 0$, то $x^{\sigma'} = x = x^{\sigma''}$ для каждого x; поэтому предположим, что $w \neq 0$.

Пусть сначала элемент x не содержится в подпространстве Fw. Из равенств (2*) вытекает существование таких чисел f, f', f'' из F, что

$$x^{\sigma'} - w = f(x^{\sigma''} - w), \quad f'w = x^{\sigma'} - x, \quad f''w = x^{\sigma''} - x.$$

Исключив из полученных равенств элементы $x^{\sigma'}$ и $x^{\sigma''}$, мы найдем, что

$$f'w + x - w = f[f''w + x - w], \text{ или } (f - 1)x = (f' - 1 - ff'' - f)w.$$

Но так как x не содержится в Fw, то $f=1$ и, следовательно, $x^{\sigma'}=x^{\sigma''}$.

Пусть теперь x содержится в Fw. Если $x=0$, то, как было отмечено выше, $0^{\sigma'}=w=0^{\sigma''}$. Поэтому можно предположить, что $x\neq 0$ и, следовательно, $Fx=Fw$. Тогда существуют такие элементы y и z, что три элемента x, y, z линейно независимы. Очевидно, что y и z не содержатся в $Fw=Fx$. Поэтому, как мы показали в предыдущем абзаце,

$$y^{\sigma'}=y^{\sigma''}=y' \text{ и } z^{\sigma'}=z^{\sigma''}=z'.$$

Отсюда и из следствия (а) мы получаем

$$F(x^{\sigma'}-y')=F(x-y)=F(x^{\sigma''}-y'),$$
$$F(x^{\sigma'}-z')=F(x-z)=F(x^{\sigma''}-z').$$

Следовательно, в F существуют такие числа h', h'', k', k'', что

$$y'-x^{\sigma''}=h''(x-y),\quad z'-x^{\sigma''}=k''(x-z),$$
$$x^{\sigma'}-y'=h'(x-y),\quad x^{\sigma'}-z'=k'(x-z).$$

После почленного сложения мы получим равенство

$$(h'+h'')(x-y)=x^{\sigma'}-x^{\sigma''}=(k'+k'')(x-z),$$

из которого, в силу линейной независимости элементов x, y, z, следует, что $h'+h''=k'+k''=0$. Но тогда $x^{\sigma'}=x^{\sigma''}$; таким образом, равенство $x^{\sigma'}=x^{\sigma''}$ справедливо при любом x. Поэтому $\tau'=\sigma'^{*}=\sigma''^{*}=\tau''$, чем и доказано утверждение (2).

(3) *Если* δ *является растяжением в* $V(B)$, *оставляющим неподвижной по крайней мере одну отличную от* 0^{*} *допустимую четверку, то* $\delta=1$.

Доказательство. Существует такая перестановка σ F-пространства A, для которой $\sigma^{*}=\delta$. В силу нашего предположения и утверждения (1), σ оставляет неподвижными 0 и еще некоторый элемент, отличный от 0. Покажем, что для такого σ справедливо следующее утверждение.

(3*) Если x и y — линейно независимые элементы F-пространства A и если $x^{\sigma}=x$, то $y^{\sigma}=y$.

Действительно, в силу следствий (а) и (в), $F(x-y)=F(x-y^{\sigma})$ и $Fy=Fy^{\sigma}$. Поэтому в F существуют такие числа f и g, что $y^{\sigma}-x=f(y-x)$ и $y^{\sigma}=gy$; отсюда $gy-x=f(y-x)$. Поскольку элементы x и y линейно независимы, из последнего равенства вытекает, что $g=f=1$, и, следовательно, $y^{\sigma}=y$. Таким образом, утверждение (3*) доказано.

Так как в линейном многообразии (F, A) существуют по крайней мере три линейно независимых элемента, то из утверждения (3*) и наших предположений непосредственно следует, что $\sigma=1$, а значит, и $\delta=1$.

(4) *Перестановка σ F-пространства A тогда и только тогда будет растяжением, когда σ^* является растяжением в $V(B)$.*

Доказательство. Выше было установлено, что если σ является растяжением в A, то σ^* будет растяжением в $V(B)$. Пусть теперь σ^* есть растяжение в $V(B)$. Тогда, в силу следствия (в), $Fr = Fr^\sigma$ для каждого r из A. Поэтому в F существует такое число $f \neq 0$ (зависящее от r), что $r = fr^\sigma$. Отображение $x^\tau = fx$ для каждого x из A является растяжением в A, которому соответствует некоторое растяжение τ^* в $V(B)$. Так как растяжения в $V(B)$ образуют группу, то $\sigma^*\tau^* = (\sigma\tau)^*$ также является растяжением в $V(B)$. Поскольку $r^{\sigma\tau} = fr^\sigma = r$, растяжение $(\sigma\tau)^*$ оставляет неподвижной по крайней мере одну допустимую четверку, отличную от 0^*. Поэтому, в силу утверждения (3), $\sigma^*\tau^* = (\sigma\tau)^* = 1$; следовательно, и $\sigma\tau = 1$, так что σ является растяжением ($x^\sigma = f^{-1}x$) линейного многообразия (F, A), что и требовалось доказать.

(5) *Перестановка σ F-пространства A тогда и только тогда будет движением, когда σ^* является движением в $V(B)$.*

Доказательство. Ранее было показано, что если σ является движением в A, то σ^* будет движением в $V(B)$. Пусть теперь σ^* есть движение в $V(B)$. Положим $0^\sigma = w$. Тогда отображение $x^\tau = x + w$ представляет собой движение в A, которому соответствует движение τ^* в $V(B)$. Но так как

$$0^{*\sigma^*} = (0^\sigma)^* = w^* = (0^\tau)^* = 0^{*\tau^*},$$

то, в силу утверждения (2), $\sigma^* = \tau^*$. Отсюда следует, что и $\sigma = \tau$, т. е. преобразование σ совпадает с движением $x^\tau = x + w$, чем и завершается доказательство утверждения (5).

(6) *Перестановка σ F-пространства A тогда и только тогда будет гомотетией, когда σ^* является гомотетией совокупности $V(B)$.*

Доказательство. Выше было отмечено, что если σ является гомотетией, то и σ^* будет гомотетией. Пусть теперь σ^* есть гомотетия совокупности $V(B)$. Положим $0^\sigma = w$ и обозначим через τ движение $x^\tau = x - w$ в линейном многообразии (F, A). Тогда τ^* будет движением в $V(B)$ и, следовательно, гомотетией совокупности $V(B)$. Поскольку множество всех гомотетий совокупности $V(B)$ образует группу, перестановка $(\sigma\tau)^* = \sigma^*\tau^*$ также будет гомотетией. Теперь заметим, что $0^{\sigma\tau} = 0$; отсюда и из утверждения (1) следует, что $(\sigma\tau)^*$ является растяжением. Поэтому, в силу утверждения (4), и перестановка $\sigma\tau$ будет растяжением и, следовательно, гомотетией. Так как τ и $\sigma\tau$ являются гомотетиями линейного многообразия (F, A), то и само σ будет гомотетией, что и требовалось доказать.

Принимая теперь во внимание замечания, сделанные перед формулировкой предложения 3, мы видим, что это предложение непосредственно следует из доказанных нами утверждений (4), (5), (6).

Замечание 2. Заметим, что при доказательстве предложения 3 мы обошлись бы без утверждения (2), если бы нам было заранее известно, что движения в $V(B)$ образуют группу.

Замечание 3. Используя результаты настоящего добавления, можно доказать, что проективное отображение линейного многообразия (F, A) на линейное многообразие (G, B) определяет изоморфизм группы гомотетий F-пространства A на группу гомотетий G-пространства B, при котором движения отображаются на движения, а растяжения — на растяжения; кроме того, можно доказать, что данное проективное отображение индуцируется некоторым полулинейным преобразованием. Мы опускаем детали этого доказательства; заметим только, что этим путем можно получить второе доказательство первой основной теоремы проективной геометрии. Читатель может заметить, что методы, используемые в настоящем добавлении при доказательстве некоторых утверждений, очень близки к тем, которые были использованы в § 1.

§ 2. Группа коллинеаций

На протяжении всего этого параграфа мы будем предполагать, что *A является F-пространством, ранг которого не меньше* 3. Тогда, как было показано в § 1, каждое автопроективное отображение F-пространства A индуцируется полулинейным преобразованием [1]). Те автопроективные отображения F-пространства A, которые индуцируются линейными преобразованиями этого пространства, мы будем называть *коллинеациями* (это определение коллинеации несколько отличается от обычного). Очевидно, что совокупность всех коллинеаций образует подгруппу Π_0 группы Π всех автопроективных отображений линейного многообразия (F, A); принимая во внимание, что каждое автопроективное отображение индуцируется полулинейным преобразованием, легко проверить, что Π_0 является нормальным делителем группы Π.

Лемма 1. *Полулинейное преобразование $\sigma = (\sigma', \sigma'')$ тогда и только тогда индуцирует коллинеацию, когда σ'' является внутренним автоморфизмом тела F.*

Доказательство. Если σ индуцирует коллинеацию, то существует такое линейное преобразование (т. е. изоморфное отображение F-пространства A самого на себя) τ, что σ и τ индуцируют одно и то же автопроективное отображение. Но в таком случае полулинейное преобразование $\sigma\tau^{-1}$ оставляет инвариантным каждое подпространство F-пространства A. Поэтому, в силу пред-

[1]) В дальнейшем, если особо не оговорено, на какое линейное многообразие отображается данное линейное многообразие данным полулинейным или линейным преобразованием, подразумевается преобразование F-пространства самого на себя. — *Прим. перев.*

ложения 3 (§ 1), в теле F существует такое число $f \neq 0$, что $a^{\sigma\tau^{-1}} = fa$ для каждого a из A. Отсюда, поскольку τ является линейным преобразованием F-пространства A, мы получаем

$$a^{\sigma'} = fa^{\tau} \text{ для каждого } a \text{ из } A.$$

Следовательно,

$$x^{\sigma''}a^{\sigma'} = (xa)^{\sigma'} = f(xa)^{\tau} = fxa^{\tau} = fxf^{-1}fa^{\tau} = fxf^{-1}a^{\sigma'},$$

так что $x^{\sigma''} = fxf^{-1}$ для каждого x из F. Таким образом, σ'' является внутренним автоморфизмом тела F.

Обратно, если σ'' есть внутренний автоморфизм тела F, то в F существует такое число $v \neq 0$, что $x^{\sigma''} = v^{-1}xv$ для каждого x из F. Определим теперь отображение ρ F-пространства A самого на себя следующим образом:

$$a^{\rho} = va^{\sigma'} \text{ для каждого } a \text{ из } A.$$

Очевидно, что ρ является автоморфизмом аддитивной группы A и что σ и ρ индуцируют одно и то же автопроективное отображение F-пространства A. Кроме того, так как

$$(xa)^{\rho} = v(xa)^{\sigma'} = vx^{\sigma''}a^{\sigma'} = v(v^{-1}xv)\,a^{\sigma'} = xva^{\sigma'} = xa^{\rho},$$

то ρ является линейным преобразованием, и, следовательно, σ индуцирует коллинеацию.

Следствие 1. *Коллинеациями тогда и только тогда исчерпываются все автопроективные отображения F-пространства A, когда каждый автоморфизм тела F является внутренним.*

Это утверждение непосредственно следует из леммы 1 и первой основной теоремы проективной геометрии (§ 1).

Поле обладает вышеуказанным свойством тогда и только тогда, когда оно не имеет никаких других автоморфизмов, кроме тождественного. Примерами таких полей являются поле рациональных чисел (а также все так называемые простые поля), поле действительных чисел и все действительно замкнутые поля, его содержащие. С другой стороны, поле комплексных чисел имеет много автоморфизмов; простым примером нетождественного автоморфизма этого поля является отображение каждого комплексного числа в сопряженное ему число. Используя теоретико-множественные методы, можно показать, что число всех автоморфизмов поля комплексных чисел равно $2^{2^{\aleph_0}}$.

Простым примером некоммутативного тела, обладающего указанным свойством, является тело кватернионов. Вообще, можно показать, что если тело F конечно над своим центром и если тождественный автоморфизм является единственным автоморфизмом центра, то каждый автоморфизм тела F является внутренним (см., например, Алберт [1]).

ИССЛЕДОВАНИЕ ГРУПП ПРЕОБРАЗОВАНИЙ ЛИНЕЙНОГО МНОГООБРАЗИЯ

В § 1 была введена группа Λ всех полулинейных преобразований линейного многообразия (F, A), ранг которого не меньше 3. Каждое полулинейное преобразование σ из Λ индуцирует некоторое автопроективное отображение σ^* этого линейного многообразия; отображение σ на σ^* является гомоморфизмом группы Λ на группу Π всех автопроективных отображений F-пространства A. Ядро этого гомоморфизма мы в § 1 обозначили через N; там же было показано, что оно состоит из всех полулинейных преобразований вида $a^\sigma = fa$, где f — произвольное отличное от 0 число из F.

Пусть теперь σ — некоторое полулинейное преобразование и ν — полулинейное преобразование вида $a^\nu = fa$, содержащееся в N. Тогда

$$x^{\sigma^{-1}\nu\sigma} = (fx^{\sigma^{-1}})^\sigma = f^\sigma x \text{ для каждого } x \text{ из } A.$$

Следовательно, σ и ν перестановочны между собой тогда и только тогда, когда $f^\sigma = f$. Так как каждое число $f \neq 0$ однозначно определяет полулинейное преобразование, содержащееся в N, то σ тогда и только тогда перестановочно с каждым полулинейным преобразованием из N, когда $f^\sigma = f$ для каждого f из F. Последнее условие эквивалентно тому, что автоморфизм тела F, составляющий компоненту полулинейного преобразования σ, является тождественным; другими словами, σ является линейным преобразованием. В теорни групп совокупность элементов группы G, перестановочных с каждым элементом некоторого подмножества S группы G, называется *централизатором* подмножества S в группе G. Используя это понятие, полученный результат можно сформулировать следующим образом.

Группа T *всех линейных преобразований является централизатором нормального делителя* N *в группе* Λ.

Обозначим теперь через Λ_0 подгруппу группы Λ, состоящую из тех полулинейных преобразований, вторая компонента которых является внутренним автоморфизмом тела F. Из леммы 1 следует, что полулинейное преобразование σ тогда и только тогда принадлежит Λ_0, когда индуцированное им автопроективное отображение σ^* является коллинеацией. Отсюда, в частности, вытекает, что Λ_0 содержит подгруппы N и T. С другой стороны, по лемме 1, для каждого полулинейного преобразования σ из Λ_0 существует такое линейное преобразование σ', что σ и σ' индуцируют одну и ту же коллинеацию. Но в таком случае, в силу предложения 3 (§ 1), $\sigma\sigma'^{-1}$ является полулинейным преобразованием вида $a^{\sigma\sigma'^{-1}} = fa$; тем самым мы показали, что

$$\Lambda_0 = \mathrm{NT}.$$

Пусть B есть некоторый базис F-пространства A; обозначим через $\Gamma = \Gamma(B)$ совокупность полулинейных преобразований σ F-пространства A, удовлетворяющих условию

$$b^\sigma = b \text{ для каждого } b \text{ из } B.$$

Очевидно, что Γ является подгруппой группы Λ. Если принять во внимание, что каждый базис F-пространства A можно одним и только одним линейным преобразованием отобразить на любой другой базис того же пространства, то легко доказать, что

$$\Lambda = T\Gamma \quad \text{и} \quad T \cap \Gamma = 1.$$

Кроме того, как легко проверить, каждое полулинейное преобразование из Γ полностью определяется своей второй компонентой, представляющей собой автоморфизм тела F, и каждый автоморфизм тела F задает единственное полулинейное преобразование, принадлежащее Γ. Таким образом, отображение полулинейного преобразования σ из Γ на его вторую компоненту, являющуюся автоморфизмом тела F, представляет собой *изоморфизм группы* Γ *на группу всех автоморфизмов тела* F.

Повидимому, не существует геометрического критерия, позволяющего установить, является ли данное автопроективное отображение коллинеацией. Однако можно дать геометрическую характеристику всей группы коллинеаций как подгруппы группы автопроективных отображений, что мы сейчас и сделаем.

Лемма 2. *Автопроективное отображение, оставляющее неподвижной каждую точку некоторой прямой, является коллинеацией.*

Доказательство. Пусть наше автопроективное отображение индуцируется полулинейным преобразованием σ, и пусть оно оставляет неподвижной каждую точку подпространства L ранга 2. Тогда σ индуцирует на F-пространстве L полулинейное преобразование, оставляющее инвариантным каждое подпространство этого пространства. Поэтому, в силу предложения 3 (§ 1), существует такое число $f \neq 0$, что $t^\sigma = ft$ для каждого t из L. Таким образом, если $t \neq 0$ — элемент из L и x — произвольное число из F, то

$$x^\sigma ft = x^\sigma t^\sigma = (xt)^\sigma = f(xt) = (fx)\, t,$$

откуда $x^\sigma f = fx$ или $x^\sigma = fxf^{-1}$. Следовательно, σ является внутренним автоморфизмом тела F, определяемым элементом f^{-1}; отсюда и из леммы 1 вытекает, что автопроективное отображение, индуцированное полулинейным преобразованием σ, будет коллинеацией.

Определение 1. *Автопроективное отображение* ν *называется перспективой, если существует такое подпространство* H F-*пространства* A, *что* $r(A/H) = 1$ *и* ν *оставляет неподвижным каждое подпространство, содержащееся в* H.

Так как $r(A) > 2$, то $r(H) \geqslant 2$. Отсюда и из леммы 2 следует, что каждая перспектива является коллинеацией. Очевидно, что в определении перспективы достаточно было бы потребовать, чтобы ν оставляло неподвижной каждую точку, принадлежащую H; поэтому H мы будем называть *гиперплоскостью неподвижных точек перспективы* ν.

Лемма 3. *Если элементы a и b F-пространства A не содержатся в подпространстве S, то существует линейное преобразование σ F-пространства A, индуцирующее перспективу и удовлетворяющее условиям $a^\sigma = b$ и $s^\sigma = s$ для каждого s из S.*

Доказательство. Из теоремы о дополнении следует существование такого подпространства T, что $A = [S + Fa + Fb] \dotplus T$. Возможны два случая.

Случай 1: $S + Fa = S + Fb$. В этом случае существует такое единственное линейное преобразование σ, что $a^\sigma = b$ и $x^\sigma = x$ для каждого x из $S + T$. Так как $S + T$ является гиперплоскостью [ибо $A = (S + T) \dotplus Fa = (S + T) \dotplus Fb$], то σ индуцирует перспективу, для которой $S + T$ будет гиперплоскостью неподвижных точек.

Случай 2: $S + Fa \neq S + Fb$. Так как элементы a и b не содержатся в S, то в этом случае $A = S \dotplus T \dotplus Fa \dotplus Fb$. Поэтому существует, и притом только одно, такое линейное преобразование σ, что $a^\sigma = b$, $b^\sigma = a$ и $x^\sigma = x$ для каждого x из $S + T$. Это линейное преобразование оставляет неподвижным каждый элемент гиперплоскости $H = S + T - F(a + b)$. Следовательно, σ индуцирует перспективу, для которой H будет гиперплоскостью неподвижных точек.

Предложение 1. *Если ν есть коллинеация и S – подпространство конечного ранга F-пространства A, то существует такое произведение π не более чем $r(S)$ перспектив F-пространства A, что $X^\nu = X^\pi$ для каждого подпространства X, содержащегося в S.*

Доказательство. Пусть σ – линейное преобразование, индуцирующее коллинеацию ν. Обозначим через $s_1, \ldots, s_n$ базис подпространства S, так что $n = r(S)$. Из леммы 3 следует существование такого линейного преобразования σ_1, индуцирующего перспективу, при котором $s_1^{\sigma\sigma_1} = s_1$. Очевидно, что $\rho_1 = \sigma\sigma_1$ является линейным преобразованием, оставляющим неподвижным каждый элемент подпространства $S_1 = Fs_1$.

Предположим теперь по индукции, что для некоторого i, $0 < i < n$, уже построены такие линейные преобразования $\sigma_1, \ldots, \sigma_i$, что каждое из них индуцирует перспективу и линейное преобразование $\rho_i = \sigma\sigma_1 \ldots \sigma_i$ оставляет неподвижным каждый элемент подпространства $S_i = \sum_{j=1}^{i} Fs_j$. Тогда элементы s_{i+1} и $s_{i+1}^{\rho_i}$ не содержатся в S_i; следовательно, по лемме 3, существует линейное

преобразование σ_{i+1}, индуцирующее перспективу, оставляющее неподвижным каждый элемент из S_i и отображающее $s_{i+1}^{\rho_i}$ на s_{i+1}. В таком случае $\rho_{i+1}=\rho_i\sigma_{i+1}$ будет линейным преобразованием, оставляющим неподвижными каждый элемент из S_i и элемент s_{i+1}, т. е. ρ_{i+1} оставляет неподвижным каждый элемент подпространства $S_{i+1}=S_i+Fs_{i+1}$.

Таким образом, методом индукции мы доказали существование таких линейных преобразований $\sigma_1, \ldots, \sigma_n$, что каждое из них индуцирует перспективу, причем линейное преобразование $\sigma\sigma_1 \ldots \sigma_n$ оставляет неподвижным каждый элемент подпространства S. Проективное отображение π, индуцированное линейным преобразованием $\sigma_n^{-1} \ldots \sigma_1^{-1}$, является произведением (самое большее) n перспектив и удовлетворяет условию $X^\nu=X^\pi$ для каждого подпространства X, содержащегося в S.

Теорема 1. *Автопроективное отображение тогда и только тогда является коллинеацией, когда его можно представить в виде произведения (не более трех) автопроективных отображений, для каждого из которых существует прямая неподвижных точек.*

Доказательство. Достаточность нашего условия непосредственно вытекает из леммы 2. Обратно, пусть σ является коллинеацией, и пусть L — произвольная прямая. Тогда, в силу предложения 1, существуют такие перспективы σ_1 и σ_2, что $P^\sigma=P^{\sigma_1\sigma_2}$ для каждой точки P, лежащей на прямой L. Отсюда следует, что $\sigma=\rho\sigma_1\sigma_2$, где ρ — автопроективное отображение, оставляющее неподвижной каждую точку прямой L; перспективы σ_1 и σ_2 обладают по крайней мере по одной прямой неподвижных точек.

Теорема 2. *Автопроективное отображение линейного многообразия конечного ранга тогда и только тогда является коллинеацией, когда оно представимо в виде произведения перспектив.*

Эта теорема непосредственно следует из леммы 2 и предложения 1.

Для линейных многообразий бесконечного ранга можно дать следующее простое истолкование предложения 1: автопроективное отображение тогда и только тогда является коллинеацией, когда его можно «аппроксимировать» произведениями перспектив. Детали доказательства этого утверждения мы оставляем читателю, интересующемуся топологией.

§ 3. Вторая основная теорема проективной геометрии

В настоящем параграфе мы будем предполагать, что A является F-пространством конечного ранга $r(A)=n$. Предположим также, что $n>1$, ибо в противном случае наше исследование было бы бессодержательным (а некоторые из доказываемых здесь утвержде-

ний при $n=1$ неверны). В то же время у нас нет никакой необходимости предполагать, что $n>2$, поскольку мы будем изучать только коллинеации, а они *по определению* индуцируются линейными преобразованиями.

Множество, состоящее из $r(A)+1$ точек, мы назовем *симплексом*, если никакие $r(A)$ точек этого множества не принадлежат одной гиперплоскости. Другими словами, любые $r(A)$ из $r(A)+1$ точек симплекса независимы. Если, например, A является плоскостью, то каждый ее симплекс состоит из четырех точек, никакие три из которых не коллинеарны.

Лемма 1. *Если точки* P_i $[i=0, 1, \ldots, r(A)]$ *образуют симплекс, то существует такой базис* $b_1, \ldots, b_n$ F*-пространства* A, *что* $P_i=Fb_i$ *для* $i=1, \ldots, n$ *и*

$$P_0=F\sum_{j=1}^{n} b_j.$$

Доказательство. Пусть b_0 — такой элемент F-пространства A, что $P_0=Fb_0$. Так как точки $P_1, \ldots, P_n$ независимы и n является рангом F-пространства A, то $A=\sum_{j=1}^{n} P_j$. Поэтому существуют такие элементы b_j, содержащиеся в соответствующих P_j, что $b_0=b_1+\ldots+b_n$. Если бы хотя бы один из элементов b_i равнялся 0, то b_0, а потому и P_0 содержались бы в гиперплоскости $\sum_{j\neq i} P_j$, что невозможно. Таким образом, $P_i=Fb_i$, и теперь из независимости точек $P_1, \ldots, P_n$ следует, что элементы $b_1, \ldots, b_n$ образуют базис F-пространства A.

Предложение 1. *Если* P_i' *и* P_i'' *— симплексы, то существует такая коллинеация* σ, *что* $P_i'^{\sigma}=P_i''$ *для* $i=0, 1, \ldots, n$.

Доказательство. Из леммы 1 следует существование в F-пространстве A таких базисов $p_1', \ldots, p_n'$ и $p_1'', \ldots, p_n''$, что $P_i'=Fp_i'$, $P_i''=Fp_i''$ для $i=1, \ldots, n$ и $P_0'=F\sum_{i=1}^{n} p_i'$, $P_0''=F\sum_{i=1}^{n} p_i''$. В таком случае существует такое однозначно определенное линейное преобразование σ F-пространства A, при котором $p_i'^{\sigma}=p_i''$ для $i=1, \ldots, n$; очевидно, что σ индуцирует требуемую коллинеацию.

Предложение 2. *Тождественная коллинеация тогда и только тогда будет единственной коллинеацией, оставляющей неподвижной каждую точку некоторого симплекса, когда* F *является полем.*

Доказательство. Пусть P_i есть некоторый симплекс F-пространства A. Тогда, по лемме 1, в A существует такой базис $b_1, \ldots, b_n$, что $P_i=Fb_i$ для $i=1, \ldots, n$ и $P_0=F\sum_{i=1}^{n} b_i$.

Предположим теперь, что лишь тождественная коллинеация оставляет неподвижной каждую точку P_i нашего симплекса. Пусть f — произвольное отличное от 0 число из F. Тогда существует такое однозначно определенное линейное преобразование σ F-пространства A, при котором $b_i^\sigma = fb_i$ для $i = 1, \ldots, n$. Это линейное преобразование индуцирует коллинеацию σ, удовлетворяющую условию $P_i^\sigma = P_i$ для $i = 0, 1, \ldots, n$. Отсюда, в силу нашего предположения, следует, что σ индуцирует тождественную коллинеацию. Рассмотрим теперь произвольный элемент z из F. Поскольку σ индуцирует тождественную коллинеацию,

$$F(b_1 + zb_2) = [F(b_1 + zb_2)]^\sigma = F(fb_1 + zfb_2) = F(b_1 + f^{-1}zfb_2).$$

Отсюда, принимая во внимание линейную независимость элементов b_1 и b_2, мы получаем, что $z = f^{-1}zf$, или $fz = zf$; так как это справедливо для любых f и z, то F является полем.

Обратно, допустим, что F есть поле, и рассмотрим некоторую коллинеацию σ, оставляющую неподвижной каждую точку P_i нашего симплекса. Коллинеация σ индуцируется некоторым линейным преобразованием, которое мы также обозначим через σ. Так как $P_i^\sigma = P_i$ для $i = 0, 1, \ldots, n$, то в F существуют такие числа $f_i \neq 0$, что

$$b_i^\sigma = f_i b_i \quad \text{для} \quad i = 1, \ldots, n, \quad \Big[\sum_{i=1}^{n} b_i\Big]^\sigma = f_0 \sum_{i=1}^{n} b_i.$$

Отсюда следует, что

$$\sum_{i=1}^{n} f_0 b_i = \sum_{i=1}^{n} b_i^\sigma = \sum_{i=1}^{n} f_i b_i,$$

и так как элементы b_i линейно независимы, то $f_0 = f_1 = \ldots = f_n$. Если теперь a — произвольный элемент F-пространства A, то, используя коммутативность поля F, мы получаем

$$a^\sigma = \Big[\sum_{i=1}^{n} a_i b_i\Big]^\sigma = \sum_{i=1}^{n} a_i f_0 b_i = f_0 \sum_{i=1}^{n} a_i b_i = f_0 a.$$

Таким образом, σ оставляет неподвижной каждую точку F-пространства A, т. е. σ является тождественным проективным отображением.

Замечание 1. Отображая точку (x_1, x_2, x_3) плоскости над полем комплексных чисел на комплексно сопряженную точку $(\bar{x}_1, \bar{x}_2, \bar{x}_3)$, мы получим автопроективное отображение, оставляющее неподвижной каждую точку симплекса (1, 1, 1), (1, 0, 0), (0, 1, 0), (0, 0, 1); в то же время при этом автопроективном отображении не остается неподвижной точка, представленная тройкой $(i, 1, 0)$, где $i^2 = -1$. Таким образом, предложение 2 перестает быть справедливым, если не ограничиваться рассмотрением лишь коллинеаций.

Замечание 2. Если ранг F-пространства A не меньше 3, то, используя первую основную теорему проективной геометрии (§ 1), можно показать, что группа всех автопроективных отображений, оставляющих неподвижной каждую точку данного симплекса, изоморфна группе автоморфизмов поля F. См. § 2, исследование групп преобразований линейного многообразия.

Замечание 3. Если F — некоммутативное тело, то, в силу предложения 2, существуют нетождественные коллинеации, оставляющие неподвижной каждую точку данного симплекса. Из теоремы 2 (§ 2) следует, что такие коллинеации представимы в виде произведения перспектив. Это показывает, что произведение перспектив может оставлять неподвижной каждую точку некоторого симплекса, не будучи тождественным.

Теперь следующим образом может быть сформулирована

Вторая основная теорема проективной геометрии. *Каждый симплекс тогда и только тогда отображается на любой другой симплекс одной и только одной коллинеацией, когда основное тело является полем.*

Эта теорема непосредственно следует из предложений 1 и 2.

Замечание 4. Результаты настоящего параграфа можно обобщить на линейные многообразия бесконечного ранга. Для этого нужно исследовать действие линейного преобразования на подпространства конечного ранга. Кроме того, необходимо найти другое определение понятия симплекса, ибо в том виде, как оно было определено в настоящем параграфе, это понятие теряет смысл в случае линейного многообразия бесконечного ранга. Мы оставляем эти рассмотрения интересующемуся читателю.

Добавление II

Теорема Паппа

Вторая основная теорема проективной геометрии (§ 3) является первым примером, показывающим, какими важными дополнительными свойствами обладает линейное многообразие, если его основное тело F является полем. В настоящем добавлении мы изложим знаменитую интерпретацию коммутативности основного тела F при помощи геометрических конфигураций, принадлежащую Гильберту.

Рассмотрим конфигурацию из десяти компланарных точек, получающуюся следующим образом (фиг. 4). На каждой из двух данных различных прямых L' и L'', пересекающихся в точке P, отмечаются по три таких различных точки P'_i (на прямой L') и P''_i (на прямой L''), что $P'_i \neq P$ и $P''_i \neq P$ для $i = 1, 2, 3$. Легко проверить, что три подпространства

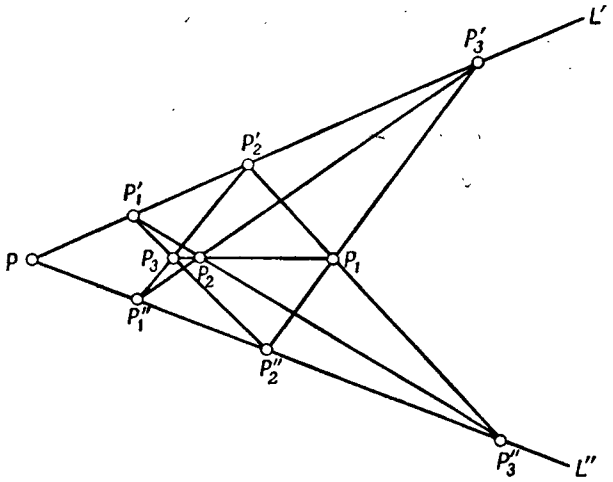
$$P_i = (P'_j + P''_k) \cap (P''_j + P'_k),$$

где i, j, k — некоторая перестановка индексов 1, 2, 3, будут точками; говорят, что *эта конфигурация* $[P_i, P'_i, P''_i]$ *обладает свойством Паппа, если точки* P_1, P_2, P_3 *коллинеарны.*

Пусть a — любой такой элемент, что $P = Fa$. Поскольку

$$P < L' = P'_1 + P'_2,$$

a можно представить в виде $a = b' - b$, где b и b' — элементы, содержащиеся соответственно в P'_1 и P'_2; так как точка P не совпадает ни с одной из точек P'_i, то b и b' отличны от 0. Поэтому



Фиг. 4.

$P'_1 = Fb$ и $P'_2 = F(a + b)$. Ввиду того, что точка P'_3 лежит на прямой $L' = P + P'_1$, мы имеем $P'_3 = F(a + d'b)$, причем $d' \neq 0, 1$, так как P'_3 отлична от точек P, P'_1, P'_2. Аналогично доказывается существование такого элемента c из A и такого числа $d'' \neq 0, 1$ из F, что $P''_1 = Fc$, $P''_2 = F(a + c)$, $P''_3 = F(a + d''c)$.

Конфигурация $[P_i, P'_i, P''_i]$ *тогда и только тогда обладает свойством Паппа, когда* $d'd'' = d''d'$.

Доказательство. Прежде всего заметим, что три элемента a, b, c линейно независимы. Поэтому $F(a + b + c)$ является точкой; очевидно, что эта точка лежит на прямой $P'_2 + P''_1 = F(a + b) + Fc$ и на прямой $P''_2 + P'_1 = F(a + c) + Fb$. Но эти прямые пересекаются в одной точке P_3; следовательно, $P_3 = F(a + b + c)$. Подобным же образом можно показать, что $P_2 = F(a + d'b + d''c)$. Наконец, заметим, что

$$(d' - 1)^{-1} d' + (d'' - 1)^{-1} = (d' - 1)^{-1} + (d'' - 1)^{-1} d''$$

и поэтому элемент

$$(d'-1)^{-1}d'(a+b)+(d''-1)^{-1}(a+d''c)=$$
$$=(d'-1)^{-1}(a+d'b)+(d''-1)^{-1}d''(a+c)$$

содержится в пересечении P_1 прямых $P_2'+P_3''=F(a+b)+F(a+d''c)$ и $P_2''+P_3'=F(a+c)+F(a+d'b)$.

Очевидно, что P_2 и P_3 являются различными точками; поэтому наша конфигурация тогда и только тогда обладает свойством Паппа, когда $P_1<P_2+P_3$. Но это включение эквивалентно следующему условию: в F существуют такие числа h и k, что

$$(d'-1)^{-1}d'(a+b)+(d''-1)^{-1}(a+d''c)=$$
$$=h(a+d'b+d''c)+k(a+b+c). \quad (1)$$

Однако, поскольку элементы a, b, c линейно независимы, числа h и k тогда и только тогда удовлетворяют уравнению (1), когда они являются решением следующей системы уравнений:

$$\left.\begin{aligned} h+k&=(d'-1)^{-1}d'+(d''-1)^{-1},\\ hd'+k&=(d'-1)^{-1}d',\\ hd''+k&=(d''-1)^{-1}d''. \end{aligned}\right\} \quad (2)$$

Таким образом, существование решения h, k системы (2) необходимо и достаточно для того, чтобы наша конфигурация обладала свойством Паппа.

Если решение h, k системы (2) существует, то, вычитая первое уравнение этой системы из двух остальных, мы получаем

$$h(d'-1)=-(d''-1)^{-1},\quad h(d''-1)=1-(d'-1)^{-1}d'=-(d'-1)^{-1},$$

откуда

$$-(d''-1)^{-1}(d'-1)^{-1}=h=-(d'-1)^{-1}(d''-1)^{-1},$$

или $(d'-1)(d''-1)=(d''-1)(d'-1)$, и, следовательно, $d'd''=d''d'$.

Обратно, если $d'd''=d''d'$, то, как легко проверить, числа

$$h=-(d''-1)^{-1}(d'-1)^{-1},\quad k=d'(d'-1)^{-1}d''(d''-1)^{-1}$$

составляют решение системы уравнений (2). Таким образом, мы показали, что равенство $d'd''=d''d'$ является необходимым и достаточным условием для того, чтобы конфигурация $[P_i, P_i', P_i'']$ обладала свойством Паппа, что и требовалось доказать.

Мы будем говорить, что в линейном многообразии (F, A), ранг которого не меньше 3, выполняется *постулат Паппа*, если в нем каждая конфигурация $[P_i, P_i', P_i'']$ обладает свойством Паппа. Если a, b, c — три линейно независимых элемента и если числа d' и d''

отличны от 0 и 1, то точки

$$P_1' = Fb,\ P_2' = F(a+b),\ P_3' = F(a+d'b) \text{ и } P_1'' = Fc,\ P_2'' = F(a+c),$$
$$P_3'' = F(a+d''c)$$

образуют конфигурацию рассмотренного выше типа. Поэтому справедливо следующее основное утверждение:

В линейном многообразии (F, A), ранг которого не меньше 3, тогда и только тогда выполняется постулат Паппа, когда F является полем.

§ 4. Проективная геометрия прямой в пространстве; сложное отношение

Прямая (т. е. линейное многообразие ранга 2), рассматриваемая как самостоятельный объект, с нашей геометрической точки зрения на линейные многообразия является не чем иным, как только множеством точек, не связанных между собой никакими соотношениями; единственным инвариантом прямой служит число ее точек (см. § 1, замечание 1 и структурную теорему проективной геометрии). Но прямая приобретает определенное геометрическое строение, если она вложена в линейное многообразие большего ранга.

Если (F, A) [1] — линейное многообразие, ранг которого не меньше 3, и L' и L'' — прямые, содержащиеся в (F, A), то, в абсолютном смысле слова, эквивалентны между собой те конфигурации, взятые соответственно на прямых L' и L'', которые переходят друг в друга при некотором взаимно однозначном отображении одной из этих прямых как множества точек на другую; с другой стороны, геометрическая эквивалентность этих конфигураций относительноо бъемлющего линейного многообразия (F, A) определяется теми соответствиями, которые индуцируются автопроективными отображениями линейного многообразия (F, A). В связи с этим возникает проблема, как охарактеризовать взаимно однозначные соответствия между точками прямых L' и L'', индуцированные автопроективными отображениями F-пространства A. Для ее решения введем понятие сложного отношения; подчеркнем, что это понятие, являющееся центральным в классической проективной геометрии, понадобится нам только для решения рассматриваемой частной проблемы.

Определение 1. *Если P, Q, R, S — четыре попарно различные точки прямой L, содержащейся в F-пространстве A, то число s из F тогда и только тогда принадлежит сложному отношению* $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}$, *когда в A существуют такие элементы*

[1]) В настоящем параграфе автор всюду предполагает, что основное тело F содержит по крайней мере 3 элемента. — *Прим. перев.*

p и q, что

$$P = Fp,\ Q = Fq,\ R = F(p+q),\ S = F(p+sq). \qquad (*)$$

Употребление для обозначения сложного отношения «квадратного» символа (введенного Ф. Леви) будет оправдано правилами симметрии, которые мы получим позже. Оправданием для употребления термина «сложное отношение» при обозначении не одного числа, а множества чисел может служить

Предложение 1. *Сложное отношение четырех попарно различных коллинеарных точек является полным классом сопряженных чисел тела* F.

Здесь в соответствии с общепринятой терминологией мы называем два числа h и k тела F *сопряженными*, если в F существует такое число $c \neq 0$, что $h = c^{-1}kc$; полный класс всех чисел, сопряженных с данным числом k из F, мы будем обозначать символом $<k>$.

Доказательство. Пусть P, Q, R, S — четыре попарно различные коллинеарные точки. Тогда

$$P+Q = P+R = P+S = Q+R = Q+S = R+S = L$$

является прямой нашего линейного многообразия (F, A). Прежде всего покажем, что существует по крайней мере одно число, принадлежащее сложному отношению $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}$. Для этого возьмем любой элемент r, удовлетворяющий условию $R = Fr$. Поскольку r принадлежит подпространству $P+Q$, существуют такие однозначно определенные элементы p и q, содержащиеся соответственно в P и Q, что $r = p+q$; ни один из элементов p и q не равен 0, так как точка R отлична от точек P и Q. Таким образом, $P = Fp$, $Q = Fq$, $R = F(p+q)$. Далее, так как элемент p содержится в подпространстве $Q+S = P+Q$, то в Q и S соответственно найдутся такие элементы q' и w, что $p = q'+w$; элементы q' и w отличны от 0, так как точка P отлична от точек Q и S. Следовательно, $Q = Fq'$ и $S = Fw$. Так как $Fq = Q = Fq'$, то существует такое число $s \neq 0$, что $q' = -sq$, и поэтому $S = Fw = F(p+sq)$. Таким образом, s принадлежит сложному отношению $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}$; заметим, что $s \neq 0, 1$.

Пусть теперь s есть некоторое фиксированное число, содержащееся в рассматриваемом сложном отношении. Тогда в F-пространстве A существуют такие элементы p и q, что

$$P = Fp,\ Q = Fq,\ R = F(p+q),\ S = F(p+sq).$$

Рассмотрим теперь число s' из F, сопряженное с s. Это означает, что в F существует такое число $t \neq 0$, что $s' = tst^{-1}$. Поэтому

точки P, Q, R, S можно представить в виде

$$P=F(tp),\ Q=F(tq),\ R=F(tp+tq),\ S=F(tp+s'(tq)),$$

откуда следует, что s' принадлежит сложному отношению $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}$. Обратно, если s' содержится в нашем сложном отношении, то в A существуют такие элементы p' и q', что

$$P=Fp',\ Q=Fq',\ R=F(p'+q'),\ S=F(p'+s'q').$$

Но тогда в F найдутся такие отличные от 0 числа h, k, m, n, что

$$p'=hp,\ q'=kq,\ p'+q'=m(p+q),\ p'+s'q'=n(p+sq).$$

Из этих равенств вытекает, что $m(p+q)=hp+kq$ и $n(p+sq)=hp+s'kq$. Отсюда, в силу линейной независимости элементов p и q, мы получаем, что $m=h=k$, $n=h$ и $ns=s'k$, откуда $s'=nsn^{-1}$, и, следовательно, s' сопряжено с s. Таким образом, сложное отношение $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}$ совпадает с совокупностью всех чисел, сопряженных с числом s, что и требовалось доказать.

Замечание 1. При доказательстве предложения мы попутно отметили тот очевидный факт, что если требовать, чтобы точки P, Q, R, S были попарно различными, то сложное отношение $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}$ не будет содержать чисел 0 и 1. Если же мы допустим, что $S=P$, то, как видно из равенств (*), это сложное отношение надо считать состоящим из одного 0; если же допустить, что $S=R$, то, также согласно равенствам (*), сложное отношение надо считать содержащим лишь 1. Эти два возможных случая мы иногда будем включать в наши рассмотрения. В то же время случай $S=Q$ недопустим, если мы не хотим вводить значение ∞, которое в этом случае содержалось бы в сложном отношении. Во всех указанных частных случаях предполагается, что точки P, Q, R попарно различны. Однако, как правило, мы будем требовать, чтобы P, Q, R, S были попарно различными точками.

Замечание 2. Пусть $P=Fp$, $Q=Fq$, $R=F(p+q)$, $S=F(p+sq)$; тогда, если $s\neq 0$, то $S=F(q+s^{-1}p)$. Это показывает, что сложное отношение $\begin{bmatrix} Q & P \\ S & R \end{bmatrix}$ состоит из всех чисел, обратных числам сложного отношения $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}$. Полученный результат можно записать в виде

$$\begin{bmatrix} P & Q \\ S & R \end{bmatrix}^{-1}=\begin{bmatrix} Q & P \\ S & R \end{bmatrix};$$

подобным же образом можно проверить, что

$$\begin{bmatrix} P & Q \\ S & R \end{bmatrix}^{-1} = \begin{bmatrix} P & Q \\ R & S \end{bmatrix}.$$

Теперь заметим, что $1 - t^{-1}st = t^{-1}(1-s)t$. Поэтому, если s пробегает полный класс сопряженных чисел, то и $1-s$ также пробегает полный класс сопряженных чисел тела F; тем самым каждому классу C сопряженных чисел можно сопоставить вполне определенный класс сопряженных чисел $1-C$. Принимая теперь во внимание, что

$$S = F(p+sq),\ P = F(-p),\ Q = F[(p+sq)+(-p)],$$
$$R = F[(p+sq)+(1-s)(-p)],$$

мы получаем

$$\begin{bmatrix} S & P \\ R & Q \end{bmatrix} = 1 - \begin{bmatrix} P & Q \\ S & R \end{bmatrix}.$$

Теперь легко подсчитать, из каких чисел состоят сложные отношения всех 24 возможных перестановок четырех точек P, Q, R, S. В частности, легко убедиться в справедливости следующей *формулы симметрии*:

$$\begin{bmatrix} P & Q \\ S & R \end{bmatrix} = \begin{bmatrix} S & R \\ P & Q \end{bmatrix} = \begin{bmatrix} Q & P \\ R & S \end{bmatrix} = \begin{bmatrix} R & S \\ Q & P \end{bmatrix}.$$

Замечание 3. Нетрудно проверить, что каждый класс сопряженных чисел тела F, отличный от $<0>$ и $<1>$, представляет собой сложное отношение некоторой четверки коллинеарных точек.

Для дальнейшего изложения нам понадобятся следующие формулы, очень похожие на известные выражения для сложных отношений в классическом случае.

Лемма 1. *Пусть p и q — два линейно независимых элемента F-пространства A.*

(а) *Если u, v, w — три различных числа из F, то*

$$\begin{bmatrix} Fq & F(p+uq) \\ F(p+wq) & F(p+vq) \end{bmatrix} = <(v-u)(w-u)^{-1}>.$$

(б) *Если h, k, m, n — четыре различных числа из F, то*

$$\begin{bmatrix} F(p+hq) & F(p+kq) \\ F(p+nq) & F(p+mq) \end{bmatrix} = <(h-n)(k-n)^{-1}(k-m)(h-m)^{-1}>.$$

Доказательство. Формула (а) непосредственно вытекает из следующих очевидных тождеств:

$$F(p+vq) = F[(v-u)q + (p+uq)],$$
$$F(p+wq) = F[(v-u)q + (v-u)(w-u)^{-1}(p+uq)].$$

Для того чтобы доказать справедливость формулы (б), убедимся сначала в справедливости такого утверждения:

(в) Если x, y, z — три различных числа из F, то

$$F(p+xq) = F[-(p+yq)+(y-x)(z-x)^{-1}(p+zq)].$$

Это утверждение вытекает из следующих тождественных соотношений:

$$(y-x)(z-x)^{-1}-1 = (y-x-z+x)(z-x)^{-1} = (y-z)(z-x)^{-1};$$

$$\begin{aligned}(y-x)(z-x)^{-1}z-y &= (y-x)(z-x)^{-1}z-z-(y-z) = \\ &= [(y-x)(z-x)^{-1}-1]z-(y-z) = \\ &= (y-z)(z-x)^{-1}z-(y-z) = \\ &= (y-z)(z-x)^{-1}[z-(z-x)] = \\ &= (y-z)(z-x)^{-1}x.\end{aligned}$$

Формула (б) следует из утверждения (в), в силу которого

$$F(p+mq) = F[-(p+hq)+(h-m)(k-m)^{-1}(p+kq)]$$

и

$$\begin{aligned}F(p+nq) &= F[-(p+hq)+(h-n)(k-n)^{-1}(p+kq)] = \\ &= F[-(p+hq)+(h-n)(k-n)^{-1}(k-m)\times \\ &\quad \times (h-m)^{-1}(h-m)(k-m)^{-1}(p+kq)].\end{aligned}$$

До сих пор наше рассмотрение сложного отношения было очень похожим на рассмотрение этого понятия в классическом случае, несмотря на то, что у нас сложное отношение представляет собой класс сопряженных чисел. Теперь мы приведем результат, который весьма отличается от классических результатов. Если P, Q, R — три попарно различные коллинеарные точки и если $<s>$ — класс сопряженных чисел тела F, то на прямой $P+Q$ всегда можно найти такую точку S, что $\begin{bmatrix} P & Q \\ S & R \end{bmatrix} = <s>$, ибо мы всегда можем найти в A такие элементы p и q, что $P = Fp$, $Q = Fq$, $R = F(p+q)$, а затем выбрать точку $S = F(p+sq)$. Но, как показывает следующее предложение, точка S в общем случае определяется точками P, Q, R и сложным отношением $<s>$ неоднозначно.

Предложение 2. *Следующие свойства четырех попарно различных точек P, Q, R, S прямой L эквивалентны:*

(I) *Если X — такая точка прямой L, что* $\begin{bmatrix} P & Q \\ S & R \end{bmatrix} = \begin{bmatrix} P & Q \\ X & R \end{bmatrix}$, *то $S = X$.*

(II) $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}$ *является одноэлементным множеством.*

(III) $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}$ *является подмножеством центра тела* F.

Доказательство. Эквивалентность свойств (II) и (III) становится очевидной, если принять во внимание, что элемент тела F тогда и только тогда принадлежит центру этого тела, когда он перестановочен с каждым элементом из F. Для того чтобы доказать эквивалентность свойств (I) и (II), заметим сначала, что существуют такие элементы p, q из A и такое число s из F, что

$$P=Fp,\quad Q=Fq,\quad R=F(p+q),\quad S=F(p+sq);\quad \begin{bmatrix} P & Q \\ S & R \end{bmatrix}=<s>.$$

Пусть справедливо свойство (I), и пусть f — произвольный отличный от 0 элемент из F. Тогда, так как при $X=F(p+f^{-1}sfq)$ мы имеем

$$\begin{bmatrix} P & Q \\ X & R \end{bmatrix}=<s>=\begin{bmatrix} P & Q \\ S & R \end{bmatrix},$$

то, ввиду (I), $F(p+f^{-1}sfq)=X=S=F(p+sq)$. Отсюда, в силу линейной независимости элементов p и q, вытекает, что $f^{-1}sf=s$. Таким образом, $<s>$ является одноэлементным множеством; этим мы показали, что свойство (II) следует из свойства (I).

Обратно, пусть справедливо свойство (II), и пусть X — такая точка, лежащая на прямой L, что $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}=\begin{bmatrix} P & Q \\ X & R \end{bmatrix}$. Поскольку точка X отлична от точки Q, ее можно представить в виде $X=F(p+xq)$. Поэтому $<s>=<x>$ и, как следует из свойства (II), $s=x$, т. е. $S=X$. Таким образом, свойство (I) следует из свойства (II), и этим предложение 2 полностью доказано.

Замечание 4. Из предложения 2 непосредственно следует, что коммутативность тела F является необходимым и достаточным условием для того, чтобы три коллинеарные точки и сложное отношение однозначно определяли четвертую точку (см. ниже теорему 2).

Замечание 5. Если характеристика тела F не равна 2, то элемент -1 отличен от 0 и 1 и содержится в центре тела F. Четыре попарно различные коллинеарные точки P, Q, R, S обычно называют *гармонической четверкой*, если $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}=-1$. Точки, составляющие гармоническую четверку, можно представить в виде

$$P=Fp,\quad Q=Fq,\quad R=F(p+q),\quad S=F(p-q).$$

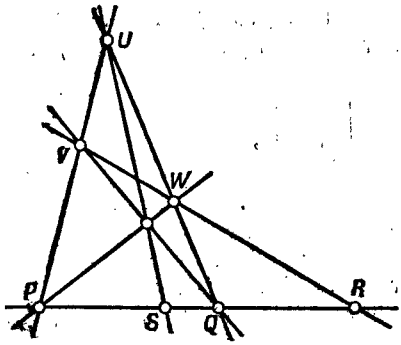
Легко проверить, что следующее условие является необходимым и достаточным для того, чтобы точки P, Q, R, S образовывали гармоническую четверку (фиг. 5):

Если точка U не лежит на прямой $P+Q$ и если V и W — такие точки, что

$$U+V=V+P=P+U,$$
$$U+W=W+Q=Q+U,$$
$$V+W=W+R=R+V,$$

то три прямые $U+S$, $W+P$, $V+Q$ пересекаются в одной точке.

Поскольку мы не хотим исключать из наших рассмотрений тела характеристики 2, мы не можем (обычно это и не нужно) отдавать предпочтение гармоническим четверкам, как это часто делают.



Фиг. 5.

Теорема 1. *Пусть P, Q, R, S и P', Q', R', S' — две четверки попарно различных коллинеарных точек.*

(а) *Тогда и только тогда существует такое автопроективное отображение π линейного многообразия (F, A), при котором $P^\pi=P'$, $Q^\pi=Q'$, $R^\pi=R'$, $S^\pi=S'$, когда существует такой автоморфизм α тела F, что* $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}^\alpha = \begin{bmatrix} P' & Q' \\ S' & R' \end{bmatrix}$.

(б) *Тогда и только тогда существует такая коллинеация σ линейного многообразия (F, A), при которой $P^\sigma=P'$, $Q^\sigma=Q'$, $R^\sigma=R'$, $S^\sigma=S'$, когда* $\begin{bmatrix} P & Q \\ S & R \end{bmatrix} = \begin{bmatrix} P' & Q' \\ S' & R' \end{bmatrix}$.

Доказательство. Прежде всего заметим, что точки первой четверки можно представить в виде

$$P=Fp,\ Q=Fq,\ R=F(p+q),\ S=F(p+sq);\ \begin{bmatrix} P & Q \\ S & R \end{bmatrix} = <s>.$$

В силу первой основной теоремы проективной геометрии (§ 1), автопроективное отображение π индуцируется некоторым полулинейным преобразованием α. Таким образом,

$$P^\pi=Fp^\alpha,\ Q^\pi=Fq^\alpha,\ R^\pi=F(p^\alpha+q^\alpha),\ S^\pi=F(p^\alpha+s^\alpha q^\alpha),$$

$$\begin{bmatrix} P^\pi & Q^\pi \\ S^\pi & R^\pi \end{bmatrix} = <s^\alpha> = <s>^\alpha = \begin{bmatrix} P & Q \\ S & R \end{bmatrix}^\alpha;$$

отсюда следует необходимость условия утверждения (а).

Обратно, если существует такой автоморфизм α тела F, что $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}^{\alpha} = \begin{bmatrix} P' & Q' \\ S' & R' \end{bmatrix}$, то $\begin{bmatrix} P' & Q' \\ S' & R' \end{bmatrix} = \langle s^{\alpha} \rangle$. Поэтому в A найдутся такие элементы p' и q', что

$$P' = Fp', \quad Q' = Fq', \quad R' = F(p' + q'), \quad S' = F(p' + s^{\alpha}q').$$

Так как p, q и p', q' — две пары линейно независимых элементов, то легко построить такое полулинейное преобразование (α, β) F-пространства A, при котором $p^{\beta} = p'$, $q^{\beta} = q'$, $(xy)^{\beta} = x^{\alpha}y^{\beta}$ для x из F и y из A [для этого нужно воспользоваться тем, что пары p, q и p', q' содержатся в некоторых, вообще говоря различных, базисах всего пространства и что любые два базиса состоят из одного и того же числа элементов (см. главу II)]. Построенное полулинейное преобразование индуцирует проективное отображение π, отображающее точки P, Q, R, S соответственно на точки P', Q', R', S'. Этим утверждение (а) доказано. Если принять во внимание, что коллинеации индуцируются линейными преобразованиями (т. е. в этом случае $\alpha = 1$), то станет ясно, что утверждение (б) доказывается точно так же, как мы доказывали утверждение (а).

Предыдущая теорема показывает, что сложное отношение характеризует четверки коллинеарных точек с точностью до проективной эквивалентности. Теперь мы займемся изучением отображений одной прямой на другую, сохраняющих все или некоторые сложные отношения. Из теоремы 1 почти непосредственно следует, что для этого достаточно рассмотреть отображения, являющиеся перестановками точек некоторой прямой, оставляющими неподвижными по крайней мере три точки.

Пусть σ есть перестановка точек прямой L, оставляющая неподвижными три различные точки U, V, W. Как мы неоднократно показывали, существуют такие линейно независимые элементы p и q, что $U = Fp$, $V = Fq$, $W = F(p + q)$. Каждую точку прямой L, отличную от V, можно однозначно представить в виде $F(p + xq)$, где x — число из F. Таким образом, элементы p и q определяют взаимно однозначное соответствие между всеми отличными от V точками прямой L и всеми элементами тела F. Отсюда следует существование такой однозначно определенной перестановки σ' чисел тела F, что

$$[F(p + xq)]^{\sigma} = F(p + x^{\sigma'}q).$$

Очевидно, что $0^{\sigma'} = 0$, $1^{\sigma'} = 1$ и что каждая перестановка σ' чисел тела F, оставляющая неподвижными 0 и 1, определяется некоторой перестановкой точек прямой L, оставляющей неподвижными точки U, V, W.

Предложение 3. *Пусть p, q — два линейно независимых элемента F-пространства A и σ — перестановка точек прямой $Fp + Fq = L$,*

оставляющая неподвижными точки Fp, Fq, $F(p+q)$; *соответствующую ей перестановку чисел тела* F *также обозначим через* σ, *так что* $[F(p+xq)]^\sigma = F(p+x^\sigma q)$ *для каждого* x *из* F. *Если число* z, *отличное от* 0 *и* 1, *содержится в центре тела* F, *то следующие свойства перестановки* σ *и числа* z *эквивалентны:*

(I) *Если* P, Q, R, S — *такие попарно различные точки прямой* L, *что* $\begin{bmatrix} P & Q \\ S & R \end{bmatrix} = z$, *то* $\begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix} = z$.

(II) *Перестановка* σ *чисел тела* F *удовлетворяет условиям:* $z^\sigma = z$ *и* $(x+y)^\sigma = x^\sigma + y^\sigma$, $(xyx)^\sigma = x^\sigma y^\sigma x^\sigma$ *для любых* x, y *из* F.

(III) σ *является автоморфизмом или инверсным автоморфизмом тела* F, *оставляющим неподвижным число* z.

Заметим, что так как элемент z содержится в центре тела F, то класс сопряженных с z элементов состоит только из одного этого элемента; поэтому z можно отождествить с классом сопряженных элементов $<z>$. Кроме того, напомним читателю, что *инверсным автоморфизмом* тела F называется такая перестановка его элементов, при которой образ суммы равен сумме образов, а образ произведения равен произведению образов, взятых в обратном порядке [т. е. $(xy)^\sigma = y^\sigma x^\sigma$].

Доказательство. Пусть справедливо свойство (I). Тогда, так как

$$\begin{bmatrix} Fp & Fq \\ F(p+zq) & F(p+q) \end{bmatrix} = z$$

и, в силу свойства (I),

$$<z^\sigma> = \begin{bmatrix} Fp & Fq \\ F(p+z^\sigma q) & F(p+q) \end{bmatrix} = \begin{bmatrix} [Fp]^\sigma & [Fq]^\sigma \\ [F(p+zq)]^\sigma & [F(p+q)]^\sigma \end{bmatrix} = z,$$

то $z^\sigma = z$. Далее, из леммы 1 (а) следует, что

$$\begin{bmatrix} Fq & Fp \\ F(p+xq) & F(p+zxq) \end{bmatrix} = z \quad \text{для каждого } x \neq 0 \text{ из } F;$$

отсюда, вновь используя свойство (I) и лемму 1 (а), мы получаем

$$z = \begin{bmatrix} Fq & Fp \\ F(p+x^\sigma q) & F(p+(zx)^\sigma q) \end{bmatrix} = <(zx)^\sigma (x^\sigma)^{-1}>.$$

Следовательно,

$$(zx)^\sigma = zx^\sigma \text{ для каждого } x \text{ из } F. \tag{I.1}$$

[Заметим, что мы выводили форму (I.1) в предположении, что $x \neq 0$, но так как $0^\sigma = 0$, то она справедлива также и для $x = 0$.]

Если u и v — два различных числа из F, то положим $w = z^{-1}(v-u)+u$; это можно сделать, поскольку $z \neq 0$. Так как $z \neq 1$, то w отлично от v; очевидно также, что w отлично от u. Принимая теперь во внимание, что z содержится в центре тела F, мы, в силу леммы 1 (а), получаем

$$\begin{bmatrix} Fq & F(p+uq) \\ F(p+wq) & F(p+vq) \end{bmatrix} = <(v-u)(w-u)^{-1}> = z.$$

Отсюда, а также из свойства (I) и леммы 1 (а) (которой можно воспользоваться, поскольку при перестановке σ различные элементы отображаются на различные элементы), вытекает, что

$$z = \begin{bmatrix} Fq & F(p+u^\sigma q) \\ F(p+w^\sigma q) & F(p+v^\sigma q) \end{bmatrix} = <(v^\sigma - u^\sigma)(w^\sigma - u^\sigma)^{-1}>.$$

Следовательно,

$$z(w^\sigma - u^\sigma) = v^\sigma - u^\sigma \text{ или } zw^\sigma = v^\sigma - u^\sigma + zu^\sigma.$$

С другой стороны, по формуле (I.1) и определению числа w,

$$zw^\sigma = (zw)^\sigma = (v-u+zu)^\sigma.$$

Таким образом, нами показано, что

$$(v-u+zu)^\sigma = v^\sigma - u^\sigma + zu^\sigma \text{ для любых } u, v \text{ из } F. \qquad (I.2)$$

[В действительности мы доказали эту формулу в предположении, что $u \neq v$; однако в случае, когда $u = v$, формула (I.2) совпадает с формулой (I.1).]

Пусть x и y — числа из F; так как $z \neq 1$, то в F существует число $u = (z-1)^{-1}y$. Из формулы (I.2) следует, что

$$(x+y)^\sigma = (x+zu-u)^\sigma = x^\sigma - u^\sigma + zu^\sigma = x^\sigma + (z-1)u^\sigma.$$

Полагая в (I.2) $v = 0$, мы получаем равенство $[(z-1)u]^\sigma = (z-1)u^\sigma$, в силу которого

$$x^\sigma + (z-1)u^\sigma = x^\sigma + [(z-1)u]^\sigma = x^\sigma + y^\sigma.$$

Тем самым показано, что

$$(x+y)^\sigma = x^\sigma + y^\sigma \text{ для любых } x \text{ и } y \text{ из } F. \qquad (I.3)$$

Теперь докажем, что если $h \neq zk$, то

$$[k(zk-h)^{-1}h]^\sigma = k^\sigma (zk^\sigma - h^\sigma)^{-1} h^\sigma. \qquad (I.4)$$

Эта формула, очевидно, справедлива, когда h или k равно 0. Поэтому можно предположить, что ни одно из чисел h и k не равно 0. Если $h = k$, то формула (I.4) превращается в равенство $[(z-1)^{-1}u]^\sigma = (z-1)^{-1}u^\sigma$, справедливость которого легко вывести из доказанного выше равенства $[(z-1)u]^\sigma = (z-1)u^\sigma$. Таким образом,

можно предположить, что $h \neq k$. Положим $m = (z-1)\,k\,(zk-h)^{-1}h$. Если бы было $m = h$, то мы имели бы $zk - h = (z-1)\,k$, откуда $h = k$, что невозможно; аналогично доказывается, что $m \neq k$. Поэтому можно воспользоваться леммой 1 (б), в силу которой

$$\begin{bmatrix} F(p+hq) & F(p+kq) \\ Fp & F(p+mq) \end{bmatrix} = \langle hk^{-1}(k-m)(h-m)^{-1}\rangle.$$

Но

$$k^{-1}(k-m) = 1 - k^{-1}m = 1 - (z-1)(zk-h)^{-1}h =$$
$$= (zk-h)^{-1}[zk - h - (z-1)h] = (zk-h)^{-1}z(k-h)$$

и, следовательно,

$$z(h-m) = z[1-(z-1)k(zk-h)^{-1}]h =$$
$$= z[(zk-h) - (z-1)k](zk-h)^{-1}h =$$
$$= z(k-h)(zk-h)^{-1}h = (zk-h+h-zh)(zk-h)^{-1}h =$$
$$= h + (1-z)h(zk-h)^{-1}h = h[1 + (1-z)(zk-h)^{-1}h] =$$
$$= h(zk-h)^{-1}[zk - h + (1-z)h] = h(zk-h)^{-1}z(k-h) = hk^{-1}(k-m),$$

откуда

$$\begin{bmatrix} F(p+hq) & F(p+kq) \\ Fp & F(p+mq) \end{bmatrix} = z.$$

Теперь, используя свойство (I) и лемму 1 (б), мы находим, что $h^\sigma(k^\sigma)^{-1}(k^\sigma - m^\sigma)(h^\sigma - m^\sigma)^{-1} = z$, или $h^\sigma(k^\sigma)^{-1}(k^\sigma - m^\sigma) = z(h^\sigma - m^\sigma)$. Из последнего равенства простым подсчетом получаем, что $m^\sigma = (z-1)\,k^\sigma(zk^\sigma - h^\sigma)^{-1}h^\sigma$, и формула (I.4) теперь непосредственно следует из равенства $[(z-1)u]^\sigma = (z-1)u^\sigma$, которым мы уже пользовались и которое легко вывести из формул (I.1) и (I.3).

Если a и b — числа из F, причем $b \neq 0$, то

$$(ab^{-1}a)^\sigma = a^\sigma(b^\sigma)^{-1}a^\sigma. \qquad (I.5)$$

Действительно, положим $k = a$ и $h = zk - b$. Тогда, поскольку $b \neq 0$, мы имеем $zk \neq h$. Поэтому можно воспользоваться формулой (I.4), из которой следует (так как $b = zk - h$), ввиду (I.1) и (I.3), что

$$[ab^{-1}(za-b)]^\sigma = [k(zk-h)^{-1}h]^\sigma = k^\sigma(zk^\sigma - h^\sigma)^{-1}h^\sigma =$$
$$= k^\sigma[(zk-h)^\sigma]^{-1}h^\sigma = a^\sigma(b^\sigma)^{-1}(za-b)^\sigma.$$

Отсюда и из формулы (I.3) вытекает, что $(ab^{-1}za)^\sigma = a^\sigma(b^\sigma)^{-1}(za)^\sigma$. Применяя теперь к последнему равенству формулу (I.1), мы убеждаемся в справедливости формулы (I.5).

Полагая в (I.5) $a = 1$ и принимая во внимание, что $1^\sigma = 1$, мы получаем равенство $(b^{-1})^\sigma = (b^\sigma)^{-1}$, опираясь на которое легко вы-

вести из формулы (I.5), что $(aba)^\sigma = a^\sigma b^\sigma a^\sigma$. Таким образом, свойство (II) следует из свойства (I).

Пусть теперь справедливо свойство (II). Тогда, полагая $a \neq 0$ и $b = a^{-1}$, мы получаем $a^\sigma = a^\sigma (a^{-1})^\sigma a^\sigma$, откуда $(a^{-1})^\sigma = (a^\sigma)^{-1}$. Полагая $b = 1$ и используя то, что $1^\sigma = 1$, мы находим, что $(a^2)^\sigma = (a^\sigma)^2$; вставляя в последнее равенство вместо a число $a + b$, мы получаем

$$(a^\sigma)^2 + a^\sigma b^\sigma + b^\sigma a^\sigma + (b^\sigma)^2 = [(a+b)^\sigma]^2 = [(a+b)^2]^\sigma =$$
$$= [a^2 + ab + ba + b^2]^\sigma = (a^2)^\sigma + (ab)^\sigma + (ba)^\sigma + (b^2)^\sigma =$$
$$= (a^\sigma)^2 + (ab)^\sigma + (ba)^\sigma + (b^\sigma)^2,$$

откуда

$$a^\sigma b^\sigma + b^\sigma a^\sigma = (ab)^\sigma + (ba)^\sigma.$$

Далее, заметим, что

$$(ba)^\sigma = [(ab)(ab)^{-1}(ba)]^\sigma = [a(b(ab)^{-1}b)a]^\sigma =$$
$$= a^\sigma [b(ab)^{-1}b]^\sigma a^\sigma = a^\sigma b^\sigma [(ab)^{-1}]^\sigma b^\sigma a^\sigma = a^\sigma b^\sigma [(ab)^\sigma]^{-1} b^\sigma a^\sigma.$$

Поэтому

$$a^\sigma b^\sigma + b^\sigma a^\sigma = (ab)^\sigma + (ba)^\sigma = (ab)^\sigma + a^\sigma b^\sigma [(ab)^\sigma]^{-1} b^\sigma a^\sigma$$

и, следовательно,

$$[(ab)^\sigma - a^\sigma b^\sigma][(ab)^\sigma]^{-1}[(ab)^\sigma - b^\sigma a^\sigma] = 0.$$

Отсюда вытекает, что для любых двух элементов a, b тела F

$$(ab)^\sigma = \begin{cases} \text{или } a^\sigma b^\sigma, \\ \text{или } b^\sigma a^\sigma. \end{cases} \tag{II.1}$$

Теперь докажем, что если a, b, c — элементы из F, то

а) или $(ab)^\sigma = a^\sigma b^\sigma$ и $(ac)^\sigma = a^\sigma c^\sigma$, или $(ab)^\sigma = b^\sigma a^\sigma$ и $(ac)^\sigma = c^\sigma a^\sigma$;
б) или $(ba)^\sigma = b^\sigma a^\sigma$ и $(ca)^\sigma = c^\sigma a^\sigma$, или $(ba)^\sigma = a^\sigma b^\sigma$ и $(ca)^\sigma = a^\sigma c^\sigma$. (II.2)

Действительно, пусть утверждение (а) неверно. Тогда без ограничения общности можно предположить, что $(ab)^\sigma \neq a^\sigma b^\sigma$. В таком случае, по формуле (II.1), $b^\sigma a^\sigma = (ab)^\sigma \neq a^\sigma b^\sigma$. Следовательно, поскольку утверждение (а) несправедливо, должно выполняться неравенство $(ac)^\sigma \neq c^\sigma a^\sigma$; поэтому, в силу формулы (II.1), $(ac)^\sigma = a^\sigma c^\sigma$. Отсюда

$$b^\sigma a^\sigma + a^\sigma c^\sigma = (ab)^\sigma + (ac)^\sigma = (ab + ac)^\sigma = [a(b+c)]^\sigma =$$
$$= \begin{cases} \text{или } a^\sigma (b+c)^\sigma = a^\sigma b^\sigma + a^\sigma c^\sigma, \\ \text{или } (b+c)^\sigma a^\sigma = b^\sigma a^\sigma + c^\sigma a^\sigma, \end{cases}$$

но оба эти возможных равенства приводят к противоречию. Следовательно, утверждение (а) справедливо; подобным же образом доказывается справедливость утверждения (б).

Если бы σ не являлось ни автоморфизмом, ни инверсным автоморфизмом тела F, то в F нашлись бы такие элементы d, e, f, g, что $(de)^\sigma \neq d^\sigma e^\sigma$ и $(fg)^\sigma \neq g^\sigma f^\sigma$. Но тогда, в силу формул (II.1) и (II.2), мы имели бы

$$(de)^\sigma = e^\sigma d^\sigma \text{ и } (dx)^\sigma = x^\sigma d^\sigma,\ (xe)^\sigma = e^\sigma x^\sigma \text{ для каждого } x \text{ из } F,$$
$$(fg)^\sigma = f^\sigma g^\sigma \text{ и } (fy)^\sigma = f^\sigma y^\sigma,\ (yg)^\sigma = y^\sigma g^\sigma \text{ для каждого } y \text{ из } F.$$

Отсюда, в частности, следует, что $(dg)^\sigma = g^\sigma d^\sigma = d^\sigma g^\sigma$ и $(fe)^\sigma = e^\sigma f^\sigma = f^\sigma e^\sigma$. Теперь, принимая во внимание формулу (II.1), мы получили бы

$$e^\sigma d^\sigma + (fe)^\sigma + (dg)^\sigma + f^\sigma g^\sigma = (de)^\sigma + (fe)^\sigma + (dg)^\sigma + (fg)^\sigma =$$
$$= [(d+f)(e+g)]^\sigma =$$
$$= \begin{cases} \text{или } (d+f)^\sigma (e+g)^\sigma = d^\sigma e^\sigma + (fe)^\sigma + (dg)^\sigma + f^\sigma g^\sigma, \\ \text{или } (e+g)^\sigma (d+f)^\sigma = e^\sigma d^\sigma + (fe)^\sigma + (dg)^\sigma + g^\sigma f^\sigma, \end{cases}$$

но каждое из этих возможных равенств приводит к противоречию. Следовательно, σ является либо автоморфизмом, либо инверсным автоморфизмом; тем самым показано, что при выполнении свойства (II) выполняется и свойство (III).

Пусть, наконец, справедливо свойство (III). Тогда, поскольку z содержится в центре тела F и $z^\sigma = z$,

$$(x+y)^\sigma = x^\sigma + y^\sigma,\ (zx)^\sigma = zx^\sigma \text{ для любых } x \text{ и } y \text{ из } F.$$

Рассмотрим теперь четыре таких попарно различных точки P, Q, R, S прямой L, для которых $\begin{bmatrix} P & Q \\ R & S \end{bmatrix} = z$. Возможны два случая.

Случай 1: одна из точек P, Q, R, S совпадает с точкой Fq. В замечании 2 было показано, что значение сложного отношения не изменяется при определенных перестановках четырех точек, причем, как легко заметить, эти перестановки образуют транзитивную группу. Поэтому без ограничения общности можно предположить, что

$$P = Fq,\ Q = F(p+uq),\ R = F(p+vq),\ S = F(p+wq).$$

Тогда, в силу леммы 1 (а),

$$(v-u)(w-u)^{-1} = z, \quad \text{т. е. } v-u = z(w-u).$$

Отсюда, используя приведенные выше свойства перестановки σ, мы получаем

$$v^\sigma - u^\sigma = (v-u)^\sigma = [z(w-u)]^\sigma = z(w-u)^\sigma = z(w^\sigma - u^\sigma)$$

и, следовательно, $(v^\sigma - u^\sigma)(w^\sigma - u^\sigma)^{-1} = z$. Поэтому, а также ввиду леммы 1 (а),

$$\begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix} = \begin{bmatrix} Fq & F(p+u^\sigma q) \\ F(p+w^\sigma q) & F(p+v^\sigma q) \end{bmatrix} = \langle (v^\sigma - u^\sigma)(w^\sigma - u^\sigma)^{-1} \rangle = z.$$

Случай 2: ни одна из точек P, Q, R, S не совпадает с точкой Fq. В этом случае наши четыре точки можно представить в виде $P = F(p+hq)$, $Q = F(p+kq)$, $R = F(p+mq)$, $S = F(p+nq)$, и, следовательно, по лемме 1 (б),

$$(h-n)(k-n)^{-1}(k-m)(h-m)^{-1} = z \qquad (*)$$

и

$$\begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix} = \langle (h^\sigma - n^\sigma)(k^\sigma - n^\sigma)^{-1}(k^\sigma - m^\sigma)(h^\sigma - m^\sigma)^{-1} \rangle. \qquad (**)$$

Если σ является автоморфизмом тела F, то из равенств (*) и (**), принимая во внимание, что σ оставляет неподвижным элемент z, мы получаем, что

$$\begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix} = z.$$

Пусть, наконец, σ является инверсным автоморфизмом тела F. Тогда заметим прежде всего, что

$$\left.\begin{aligned} &1 - [(h-n)(k-n)^{-1} - 1][(h-n)(h-m)^{-1} - 1] = \\ &= (h-n)(k-n)^{-1} + (h-n)(h-m)^{-1} - \\ &\qquad - (h-n)(k-n)^{-1}(h-n)(h-m)^{-1} = \\ &= (h-n)[(k-n)^{-1}(h-m) + 1 - (k-n)^{-1}(h-n)](h-m)^{-1} = \\ &= (h-n)(k-n)^{-1}[(h-m) + (k-n) - (h-n)](h-m)^{-1} = \\ &\qquad = (h-n)(k-n)^{-1}(k-m)(h-m)^{-1}. \end{aligned}\right\} \quad (+)$$

Поскольку последнее выражение, в силу равенства (*), совпадает с элементом z, содержащимся в центре тела F, и так как из равенства $z = 1 - uv$ следует равенство $z = u^{-1}(1-uv)u = 1 - vu$, то

$$\begin{aligned} z &= (h-n)(k-n)^{-1}(k-m)(h-m)^{-1} = \\ &= 1 - [(h-n)(k-n)^{-1} - 1][(h-n)(h-m)^{-1} - 1] = \\ &= 1 - [(h-n)(h-m)^{-1} - 1][(h-n)(k-n)^{-1} - 1] = \\ &= 1 - [(n-h)(m-h)^{-1} - 1][(n-h)(n-k)^{-1} - 1] = \qquad [\text{ввиду } (+)] \\ &= (n-h)(m-h)^{-1}(m-k)(n-k)^{-1} = \\ &= (h-n)(h-m)^{-1}(k-m)(k-n)^{-1} = \\ &= (h-m)^{-1}(k-m)(k-n)^{-1}(h-n); \end{aligned}$$

последнее равенство вытекает из того, что так как элемент z содержится в центре тела F, то он не меняется при трансформировании его элементом $(h-n)$. Теперь из равенства (**), учитывая, что σ оставляет неподвижным элемент z, мы получаем

$$\begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix} = <[(h-m)^{-1}(k-m)(k-n)^{-1}(h-n)]^\sigma> = z.$$

Таким образом, мы показали, что свойство (I) следует из свойства (III); этим предложение 3 полностью доказано.

Замечание 6. При доказательстве того, что из свойства (II) следует свойство (III), мы по существу доказали справедливость следующего утверждения.

Перестановка σ элементов тела F тогда и только тогда является автоморфизмом или инверсным автоморфизмом тела F, когда

$$1^\sigma = 1, \quad (x+y)^\sigma = x^\sigma + y^\sigma, \quad (xyx)^\sigma = x^\sigma y^\sigma x^\sigma.$$

Такие перестановки σ элементов тела F называются *полуавтоморфизмами* тела F.

Приведенное доказательство того, что каждый полуавтоморфизм есть либо автоморфизм, либо инверсный автоморфизм, взято из работы Хуа Ло-гэна [2]. Более поздние результаты, относящиеся к общей проблеме полуавтоморфизмов, читатель найдет в работе Джекобсона — Рикарта [1].

Замечание 7. Если ограничиться рассмотрением частного случая $z = -1$ (который невозможен только тогда, когда характеристика тела F равна 2), то наше исследование сведется к изучению перестановок точек прямой, отображающих гармонические четверки (см. замечание 5) на гармонические четверки, и приведет к обобщению известной теоремы Штаудта. В связи с этим см. ниже предложение 4, а также работу Анкочея [1], в которой можно найти дальнейшие ссылки на имеющуюся литературу.

Введем теперь понятие, обобщающее то соотношение между перестановками точек прямой и перестановками чисел основного тела, которое было использовано в предложении 3. Пусть σ есть взаимно однозначное отображение совокупности всех точек прямой L на совокупность всех точек прямой L^σ. Перестановку τ чисел основного тела F мы назовем *σ-допустимой*, если существуют такие пары линейно независимых элементов p, q и p', q', содержащиеся соответственно в L и L^σ, что

$$(Fp)^\sigma = Fp', \quad [F(p+q)]^\sigma = F(p'+q'), \quad (Fq)^\sigma = Fq',$$
$$[F(p+xq)]^\sigma = F(p'+x^\tau q') \text{ для каждого } x \text{ из } F.$$

Из этих равенств непосредственно следует, что $0^\tau = 0$ и $1^\tau = 1$.

Заметим, что перестановка σ чисел тела F, о которой шла речь в предложении 3, была допустимой относительно перестановки σ точек прямой L. Легко видеть, что для каждого взаимно однозначного отображения σ точек прямой L на точки прямой L^σ существует по крайней мере одна σ-допустимая перестановка тела F. Легко видеть также, что любая перестановка элементов тела F, оставляющая неподвижными 0 и 1, определяет (и притом в большом числе) взаимно однозначные отображения точек одной прямой на точки некоторой другой прямой, относительно которых данная перестановка является допустимой.

Лемма 2. *Если σ есть взаимно однозначное отображение совокупности точек прямой L на совокупность точек прямой L^σ и если полуавтоморфизм α тела F σ-допустим, то*

$$\begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix} = \begin{bmatrix} P & Q \\ S & R \end{bmatrix}^\alpha$$

для любых четырех попарно различных точек P, Q, R, S прямой L.

Доказательство. Так как полуавтоморфизм α является σ-допустимым, то существуют такие элементы p, q, p', q', что

$$L = Fp + Fq,\ L^\sigma = Fp' + Fq',$$
$$(Fp)^\sigma = Fp',\ [F(p+q)]^\sigma = F(p'+q'),\ (Fq)^\sigma = Fq',$$
$$[F(p+xq)]^\sigma = F(p' + x^\alpha q') \text{ для каждого } x \text{ из } F.$$

Теперь мы будем доказывать нашу лемму совершенно так же, как в предложении 3 доказывалось, что из свойства (III) следует свойство (I). Пусть P, Q, R, S — четыре попарно различные точки прямой L. Возможны два случая.

Случай 1: одна из наших четырех точек совпадает с точкой Fq. Тогда без ограничения общности можно предположить, что $P = Fq$ и $Q = F(p+uq)$, $R = F(p+vq)$, $S = F(p+wq)$, где u, v, w — три различных числа из F. Поэтому можно воспользоваться леммой 1 (а), из которой вытекает, что

$$\begin{bmatrix} P & Q \\ S & R \end{bmatrix} = \langle (v-u)(w-u)^{-1} \rangle,\ \begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix} = \langle (v^\alpha - u^\alpha)(w^\alpha - u^\alpha)^{-1} \rangle.$$

Но α является либо автоморфизмом, либо инверсным автоморфизмом тела F; числа же xy^{-1} и $y^{-1}x = y^{-1}(xy^{-1})y$ сопряжены в F. Следовательно,

$$\langle (v^\alpha - u^\alpha)(w^\alpha - u^\alpha)^{-1} \rangle = \langle [(v-u)(w-u)^{-1}]^\alpha \rangle,$$

откуда

$$\begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix} = \begin{bmatrix} P & Q \\ S & R \end{bmatrix}^\alpha.$$

Случай 2: ни одна из точек P, Q, R, S не совпадает с точкой Fq. В этом случае наши точки можно представить в виде

$$P = F(p + hq),\ Q = F(p + kq),\ R = F(p + mq),\ S = F(p + nq),$$

где h, k, m, n — четыре различных числа из F. В силу леммы 1 (б),

$$\begin{bmatrix} P & Q \\ S & R \end{bmatrix} = \langle (h-n)(k-n)^{-1}(k-m)(h-m)^{-1} \rangle,$$

$$\begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix} = \langle (h^\alpha - n^\alpha)(k^\alpha - n^\alpha)^{-1}(k^\alpha - m^\alpha)(h^\alpha - m^\alpha)^{-1} \rangle.$$

При доказательстве последней части предложения 3 мы установили, что

$$(h-n)(k-n)^{-1}(k-m)(h-m)^{-1} = 1 - [(h-n)(k-n)^{-1} - 1][(h-n)(h-m)^{-1} - 1] = t; \quad (*)$$

при помощи тождества (*) было показано, что число t сопряжено в F с числом

$$t' = 1 - [(h-n)(h-m)^{-1} - 1][(h-n)(k-n)^{-1} - 1] = 1 - [(n-h)(m-h)^{-1} - 1][(n-h)(n-k)^{-1} - 1] = (n-h)(m-h)^{-1}(m-k)(n-k)^{-1},$$

и там же была показана сопряженность в F числа t' с числом

$$t'' = (m-h)^{-1}(m-k)(n-k)^{-1}(n-h) = (h-m)^{-1}(k-m)(k-n)^{-1}(h-n),$$

которое получается из t изменением порядка его множителей на обратный. Отсюда следует, что

$$\langle (h-n)(k-n)^{-1}(k-m)(h-m)^{-1} \rangle = \langle (h-m)^{-1}(k-m)(k-n)^{-1}(h-n) \rangle. \quad (**)$$

Если теперь α — автоморфизм, то мы воспользуемся левой частью равенства (**); если же α — инверсный автоморфизм, то воспользуемся правой частью равенства (**). В обоих случаях получаем, что

$$\begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix} = \langle (h^\alpha - n^\alpha)(k^\alpha - n^\alpha)^{-1}(k^\alpha - m^\alpha)(h^\alpha - m^\alpha)^{-1} \rangle = \begin{bmatrix} P & Q \\ S & R \end{bmatrix}^\alpha;$$

тем самым лемма полностью доказана.

Предложение 4. *Если σ есть взаимно однозначное отображение совокупности точек прямой L на совокупность точек прямой L^σ и если центр тела F содержит по крайней мере три элемен-*

та, то σ тогда и только тогда сохраняет все сложные отношения, когда σ-допустимые перестановки тела F являются полуавтоморфизмами, оставляющими инвариантным каждый класс сопряженных элементов тела F.

Доказательство. Достаточность нашего условия непосредственно следует из леммы 2. Обратно, предположим, что отображение σ сохраняет все сложные отношения, и рассмотрим σ-допустимую перестановку τ элементов тела F. Существуют такие две пары линейно независимых элементов p, q и p', q', содержащиеся соответственно в L и L^σ, что

$$(Fp)^\sigma = Fp', \quad [F(p+q)]^\sigma = F(p'+q'), \quad (Fq)^\sigma = Fq',$$
$$[F(p+xq)]^\sigma = F(p'+x^\tau q') \text{ для каждого } x \text{ из } F.$$

Очевидно, что найдется такое линейное преобразование η F-пространства L^σ на F-пространство L, при котором $(xp'+yq')^\eta = xp+yq$ для любых x и y из F. Это линейное преобразование индуцирует взаимно однозначное отображение σ′ совокупности точек прямой L^σ на совокупность точек прямой L; легко проверить, используя лемму 1 или лемму 2, что σ′ сохраняет сложные отношения. Поэтому σσ′ является перестановкой точек прямой L, сохраняющей сложные отношения; кроме того, совершенно очевидно, что эта перестановка обладает следующими свойствами:

$$(Fp)^{\sigma\sigma'} = Fp, \quad [F(p+q)]^{\sigma\sigma'} = F(p+q), \quad (Fq)^{\sigma\sigma'} = Fq,$$
$$[F(p+xq)]^{\sigma\sigma'} = F(p+x^\tau q) \text{ для каждого } x \text{ из } F.$$

В силу наших предположений, в центре тела F существует число z, отличное от 0 и 1. Таким образом, поскольку перестановка σσ′ сохраняет все сложные отношения, выполнены все условия утверждения (I) предложения 3, откуда вытекает, что τ является полуавтоморфизмом. Так как, кроме того, справедливы равенства

$$\langle x\rangle = \begin{bmatrix} Fp & Fq \\ F(p+xq) & F(p+q) \end{bmatrix} = \begin{bmatrix} Fp & Fq \\ F(p+x^\tau q) & F(p+q) \end{bmatrix} = \langle x^\tau\rangle$$

для каждого числа x из F, то полуавтоморфизм τ оставляет инвариантным каждый класс сопряженных элементов тела F. Таким образом, предложение 4 доказано.

Замечание 8. Если σ есть полуавтоморфизм тела F, оставляющий инвариантным каждый класс сопряженных элементов, то σ оставляет неподвижным каждый элемент центра Z тела F. Если σ — автоморфизм тела F, оставляющий неподвижным каждый элемент его центра Z и если F конечно над Z, то, в силу известной теоремы, σ является внутренним автоморфизмом

тела F [1]). Но если тело F бесконечно над своим центром Z, то существуют автоморфизмы тела F, оставляющие инвариантным каждый класс сопряженных элементов и не являющиеся внутренними автоморфизмами тела F. Такой пример можно найти в работе Кёте [1]. Если F конечно над Z и σ является инверсным автоморфизмом тела F, оставляющим неподвижным каждый элемент центра Z, то элементы x и x^σ для любого x из F будут корнями одних и тех же уравнений над Z. Отсюда следует сопряженность элементов x и x^σ в теле F [см., например, Артин, Несбитт, Тролл [1], стр. 67, теорема 7.2 E]. Примером такого инверсного автоморфизма является отображение каждого действительного кватерниона $x_0 + x_1 i + x_2 j + x_3 k$ на «сопряженный» ему кватернион $x_0 - x_1 i - x_2 j - x_3 k$. Все это показывает, что полуавтоморфизм, оставляющий инвариантным каждый класс сопряженных элементов, может быть либо внутренним автоморфизмом, либо автоморфизмом, не являющимся внутренним, либо инверсным автоморфизмом, не являющимся автоморфизмом. Отсюда следует, что условие инвариантности сложного отношения не является достаточным для того, чтобы отличать друг от друга те классы отображений точек прямой, относительно которых допустимыми перестановками основного тела F являются соответственно внутренние автоморфизмы, автоморфизмы, не являющиеся внутренними, и инверсные автоморфизмы.

Теорема 2. *Тело F тогда и только тогда коммутативно, когда тождественная перестановка является единственной перестановкой точек прямой, сохраняющей сложные отношения и оставляющей неподвижными по крайней мере три точки этой прямой.*

Эта теорема является своего рода дополнением ко второй основной теореме проективной геометрии (§ 3), и в то же время она уточняет замечание 4.

Доказательство. Допустим сначала, что единственной перестановкой точек прямой, сохраняющей сложные отношения и обладающей тремя неподвижными точками, является тождественная перестановка. Если g — отличное от 0 число из F и p, q — два линейно независимых элемента F-пространства A, то можно следующим образом определить перестановку σ точек прямой $L = Fp + Fq$:

$$(Fq)^\sigma = Fq, \quad [F(p + xq)]^\sigma = F(p + g^{-1}xgq) \text{ для каждого } x \text{ из } F.$$

Очевидно, что σ оставляет неподвижными три попарно различные точки: Fp, Fq, $F(p+q)$; так как отображение $x \to g^{-1}xg$ является внутренним автоморфизмом тела F, то, по лемме 2, σ

[1]) См., например, Чеботарев Н. Г. [1], стр. 59. — *Прим. перев.*

сохраняет сложные отношения. Следовательно, в силу сделанного предположения, $\sigma = 1$. Поэтому элемент $p + g^{-1}xgq$ содержится в $F(p + xq)$ для каждого x из F. Отсюда и из линейной независимости элементов p и q вытекает, что $x = g^{-1}xg$ для каждого x из F; таким образом, g содержится в центре тела F. Этим мы показали, что каждый элемент тела F содержится в центре, т. е. что F является полем.

Обратно, пусть F есть поле. Если F содержит только два элемента 0 и 1, то на прямой лежат лишь три точки и, следовательно, перестановка точек такой прямой, оставляющая неподвижными три точки, будет тождественной. Поэтому можно предположить, что F содержит по крайней мере три элемента. Рассмотрим теперь произвольную перестановку σ точек прямой L, сохраняющую сложные отношения и оставляющую неподвижными три точки. Эти неподвижные относительно σ точки можно представить в виде Fp, $F(p+q)$, Fq. Существует такая σ-допустимая перестановка τ чисел поля F, что

$$[F(p+xq)]^{\sigma} = F(p + x^{\tau}q)$$

для каждого x из F. В силу предложения 4, τ является полуавтоморфизмом поля F, оставляющим инвариантным каждый класс сопряженных элементов. Но поле F коммутативно; поэтому $\tau = 1$ и, следовательно, $\sigma = 1$, что и требовалось доказать.

Замечание 9. Легко видеть, что условия теоремы 2 эквивалентны следующему условию.

Взаимно однозначные отображения σ' и σ'' совокупности точек прямой L на совокупность точек прямой L' совпадают тогда и только тогда, когда

(а) существуют такие три попарно различные точки P_i $(i = 1, 2, 3)$ прямой L, что $P_i^{\sigma'} = P_i^{\sigma''}$ для $i = 1, 2, 3$, и

(б) $\begin{bmatrix} P^{\sigma'} & Q^{\sigma'} \\ S^{\sigma'} & R^{\sigma'} \end{bmatrix} = \begin{bmatrix} P^{\sigma''} & Q^{\sigma''} \\ S^{\sigma''} & R^{\sigma''} \end{bmatrix}$ для любых четырех попарно различных точек P, Q, R, S прямой L.

Предложение 5. *Если характеристика тела F отлична от 2 (так что $+1 \neq -1$), то следующие свойства взаимно однозначного отображения σ точек прямой L на точки прямой L^{σ} эквивалентны:*

(I) $\begin{bmatrix} P & Q \\ S & R \end{bmatrix} = \begin{bmatrix} P' & Q' \\ S' & R' \end{bmatrix}$ *тогда и только тогда, когда*

$$\begin{bmatrix} P^{\sigma} & Q^{\sigma} \\ S^{\sigma} & R^{\sigma} \end{bmatrix} = \begin{bmatrix} P'^{\sigma} & Q'^{\sigma} \\ S'^{\sigma} & R'^{\sigma} \end{bmatrix}.$$

(II) *Если P, Q, R, S—гармоническая четверка точек, то четверка точек P', Q', R', S' тогда и только тогда гармоническая,*

когда

$$\begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix} = \begin{bmatrix} P'^\sigma & Q'^\sigma \\ S'^\sigma & R'^\sigma \end{bmatrix}.$$

(III) *σ-допустимые перестановки тела F являются полуавтоморфизмами.*

Доказательство. Так как гармоническая четверка точек характеризуется тем, что ее сложное отношение равно -1, то очевидно, что свойство (II) следует из свойства (I). Пусть теперь справедливо свойство (II), и пусть P, Q, R, S—некоторая гармоническая четверка точек. Если W—такая точка прямой L^σ, что

$$\begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix} = \begin{bmatrix} P^\sigma & Q^\sigma \\ W & R^\sigma \end{bmatrix},$$

то на прямой L найдется такая единственная точка V, для которой $V^\sigma = W$. В силу свойства (II), точки P, Q, R, V составляют гармоническую четверку. Отсюда, используя предложение 2, мы получаем, что $V = S$ и, следовательно, $W = S^\sigma$. Таким образом, в силу того же предложения 2, сложное отношение $\begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix}$ состоит из одного элемента z, содержащегося в центре тела F. Так как одновременно с точками P, Q, R, S гармоническую четверку образуют точки P, Q, S, R, то, по свойству (II),

$$z = \begin{bmatrix} P^\sigma & Q^\sigma \\ S^\sigma & R^\sigma \end{bmatrix} = \begin{bmatrix} P^\sigma & Q^\sigma \\ R^\sigma & S^\sigma \end{bmatrix} = z^{-1},$$

откуда $z = \pm 1$. Но так как σ отображает четыре попарно различные точки P, Q, R, S на четыре попарно различные точки, то $z \neq 1$; тем самым доказано, что при отображении σ образом гармонической четверки является гармоническая четверка. Теперь совершенно так же, как при доказательстве предложения 4, мы из предложения 3 выводим, что σ-допустимые перестановки тела F являются полуавтоморфизмами. Таким образом, свойство (III) следует из свойства (II). Справедливость же свойства (I), при условии справедливости свойства (III), непосредственно вытекает из леммы 2.

Лемма 3. *Если σ есть взаимно однозначное отображение точек прямой L на точки прямой L^σ, то*

(а) *σ тогда и только тогда индуцируется автопроективным отображением F-пространства A, когда σ-допустимые перестановки тела F являются автоморфизмами,*

(б) *σ тогда и только тогда индуцируется коллинеацией F-пространства A, когда σ-допустимые перестановки тела F являются внутренними автоморфизмами.*

Лемма становится очевидной, если вспомнить, что, в силу первой основной теоремы проективной геометрии (§ 1), проективные отображения индуцируются полулинейными преобразованиями и что, по лемме 1 (§ 2), полулинейное преобразование тогда и только тогда индуцирует коллинеацию, когда его компонента, являющаяся автоморфизмом тела F, будет внутренним автоморфизмом.

Если σ-допустимые перестановки тела F являются инверсными автоморфизмами, которые в то же время не являются автоморфизмами, то σ не индуцируется автопроективным отображением. Тем не менее такие отображения можно некоторым способом получить из автодуальных отображений линейного многообразия; теория автодуальных отображений будет изложена в следующей главе. Читатель, интересующийся этим вопросом, сможет познакомиться с ним в добавлении II к гл. IV.

Из замечания 8 следует, что сохранение сложных отношений не является достаточным условием для того, чтобы охарактеризовать те взаимно однозначные отображения точек прямой, которые индуцируются автопроективными отображениями линейного многообразия. Поэтому возникает необходимость в некотором обобщении понятия сложного отношения.

Если P, Q, R—три попарно различные точки прямой L, то их можно представить в виде $P = Fp$, $Q = Fq$, $R = Fr$, причем $p + q + r = 0$. Если ни одна из точек X, Y, Z прямой L не совпадает с точкой Q, то эти точки можно однозначно представить в виде $X = F(p + xq)$, $Y = F(p + yq)$, $Z = F(p + zq)$. Пусть теперь выбрано другое возможное представление точек P, Q, R: $P = Fp'$, $Q = Fq'$, $R = Fr'$, причем элементы p', q', r' удовлетворяют тому же равенству $p' + q' + r' = 0$. Тогда в теле F найдется такое число $g \neq 0$, что $p' = gp$, $q' = gq$, $r' = gr$. Поэтому точки X, Y, Z можно представить в виде

$$X = F(p' + gxg^{-1}q'), \quad Y = F(p' + gyg^{-1}q'), \quad Z = F(p' + gzg^{-1}q').$$

Таким образом, второе представление точек P, Q, R приводит нас к сопряженной с (x, y, z) тройке

$$g(x, y, z)g^{-1} = (gxg^{-1}, gyg^{-1}, gzg^{-1})$$

чисел из F. Легко видеть, что, перебирая для точек P, Q, R все возможные представления указанного типа, мы получаем полный класс сопряженных троек чисел тела F. Обозначив через $<(x, y, z)>$ совокупность всех троек вида $g(x, y, z)g^{-1}$, где g—произвольное отличное от 0 число из F, мы введем

Определение 2. $\begin{bmatrix} Fp & Fq & F(p+q) \\ F(p+xq) & F(p+yq) & F(p+zq) \end{bmatrix} = <(x,y,z)>$.

Заметим, что $\begin{bmatrix} P & Q & R \\ X & Y & Z \end{bmatrix}$ определено всякий раз, когда точки

P, Q, R, X, Y, Z коллинеарны, точки P, Q, R попарно различны и ни одна из точек X, Y, Z не совпадает с Q. Кроме того, если

$$\begin{bmatrix} P & Q & R \\ X & Y & Z \end{bmatrix} = \langle (x, y, z) \rangle,$$

то

$$\begin{bmatrix} P & Q \\ X & R \end{bmatrix} = \langle x \rangle, \quad \begin{bmatrix} P & Q \\ Y & R \end{bmatrix} = \langle y \rangle, \quad \begin{bmatrix} P & Q \\ Z & R \end{bmatrix} = \langle z \rangle;$$

но обратное утверждение, вообще говоря, неверно[1]), за исключением того случая, когда все три числа x, y, z содержатся в центре тела F.

Предложение 6. *Если центр тела F содержит по крайней мере три элемента и если σ есть взаимно однозначное отображение точек прямой L на точки прямой L^σ, то σ тогда и только тогда индуцируется автопроективным отображением F-пространства A, когда существует такой автоморфизм α тела F, что*

$$\begin{bmatrix} P^\sigma & Q^\sigma & R^\sigma \\ X^\sigma & Y^\sigma & Z^\sigma \end{bmatrix} = \begin{bmatrix} P & Q & R \\ X & Y & Z \end{bmatrix}^\alpha$$

для любых (допустимых) систем точек P, Q, R, X, Y, Z прямой L.

Доказательство. Поскольку необходимость условия очевидна, ограничимся доказательством его достаточности. Если условие нашего предложения выполнено, то существует такая σ-допустимая перестановка τ тела F, что

$$\langle (x^\tau, y^\tau, z^\tau) \rangle = \langle (x^\alpha, y^\alpha, z^\alpha) \rangle \text{ для любых } x, y, z \text{ из } F.$$

Отсюда, как легко заметить, следует, что $\tau\alpha^{-1}$ является σ'-допустимой перестановкой тела F, где σ'—легко конструируемая перестановка точек прямой L, сохраняющая сложные отношения и оставляющая неподвижными по крайней мере три точки. Следовательно, в силу предложения 3, $\tau\alpha^{-1}$ является полуавтоморфизмом тела F, который мы обозначим через β, причем таким, что тройка чисел (x, y, z) сопряжена с тройкой $(x^\beta, y^\beta, z^\beta)$. Отсюда, в частности, вытекает существование для каждой пары элементов x и y из F такого элемента $g \neq 0$ из F, что

$$x^\beta = g^{-1}xg, \quad y^\beta = g^{-1}yg, \quad (xy)^\beta = g^{-1}xyg.$$

Но в таком случае

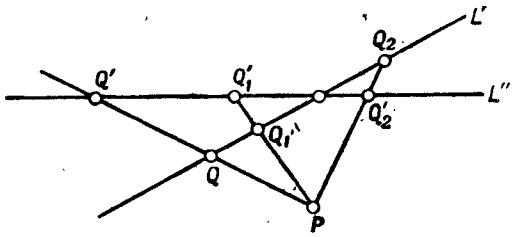
$$(xy)^\beta = g^{-1}xgg^{-1}yg = x^\beta y^\beta.$$

---

[1]) То есть не всякая тройка чисел (x', y', z'), где $x' \in \langle x \rangle$, $y' \in \langle y \rangle$ и $z' \in \langle z \rangle$, принадлежит $\langle (x, y, z) \rangle$.—*Прим. перев.*

и, следовательно, β—автоморфизм тела F. Так как α также является автоморфизмом тела F, то и τ представляет собой автоморфизм тела F. Поэтому, в силу леммы 3, σ индуцируется автопроективным отображением F-пространства A.

Соображения, приведенные в замечании 8, показывают, что хотя с помощью нашего нового понятия можно охарактеризовать все отображения точек прямой, индуцированные автопроективными отображениями, тем не менее, за исключением отдельных частных



Фиг. 6.

случаев, это понятие не является достаточным для описания отображений совокупности точек прямой, индуцированных коллинеациями. Однако в множестве всех взаимно однозначных отображений точек прямой все же можно выделить отображения, индуцированные коллинеациями; для того, чтобы это сделать, воспользуемся следующим геометрическим построением (фиг. 6).

Пусть L' и L''—прямые, расположенные в одной и той же плоскости F-пространства A, и P—некоторая точка этой плоскости, не лежащая ни на одной из прямых L' и L''. Тогда подпространство $L'+P=L''+P$ совпадает с той плоскостью, на которой расположены прямые L' и L''. Если Q'—точка прямой L', то, в силу формулы для ранга (б) (гл. II, § 2), $Q''=L''\cap(P+Q')$ является точкой прямой L''. По той же причине $L'\cap(P+Q'')$ будет точкой прямой L' для любой точки Q'' прямой L''. Эти две операции, каждая из которых ставит в соответствие точке одной из прямых точку другой прямой, являются взаимно обратными, ибо из закона Дедекинда следует, что

$$L'\cap(P+[L''\cap(P+Q')])=L'\cap(P+L'')\cap(P+Q')=$$
$$=L'\cap(P+Q')=Q',$$

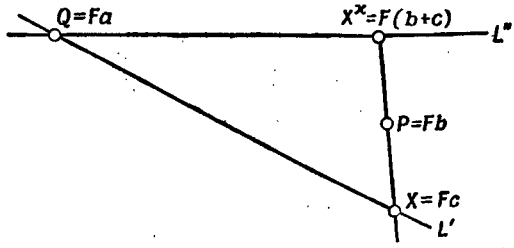
поскольку $L'<P+L''$. Отсюда, в частности, вытекает, что отображение каждой точки Q' прямой L' на точку $L''\cap(P+Q')$ прямой L'' является взаимно однозначным отображением совокупности всех точек прямой L' на совокупность всех точек прямой L''; такое отображение называется *проектированием прямой L' из*

точки P на прямую L''. (Заметим, что если $L'=L''$, то проектирование является тождественным отображением.)

Пусть теперь $L_0, L_1, \ldots, L_k$ будут прямыми F-пространства A, причем для каждого $i=0, 1, \ldots, k-1$ прямые L_i и L_{i+1} компланарны. Если P_i—такая точка F-пространства A, не лежащая на прямых L_i и L_{i+1}, что $L_i+P_i=P_i+L_{i+1}$, то можно определить проектирование σ_i прямой L_i из точки P_i на прямую L_{i+1}. Произведение $\sigma=\sigma_0\sigma_1\ldots\sigma_{k-1}$ представляет собой взаимно однозначное отображение совокупности точек прямой L_0 на совокупность точек прямой L_k. Такое отображение σ мы будем называть *линейным отображением прямой L_0 на прямую L_k.* (В литературе употребляются различные названия для того, что мы исключительно из алгебраических соображений назвали линейным отображением.)

Предложение 7. *Отображение σ точек прямой L' на точки прямой L'' линейно тогда и только тогда, когда σ индуцируется коллинеацией F-пространства A.*

Доказательство. Покажем сначала, что каждое линейное отображение индуцируется коллинеацией. Поскольку каждое линейное отображение разлагается в произведение проектирований,



Фиг. 7.

а произведение коллинеаций само является коллинеацией, нам достаточно доказать, что каждое проектирование индуцируется коллинеацией. Рассмотрим поэтому (фиг. 7) две различные компланарные прямые L', L'' и точку P, принадлежащую плоскости $L'+L''$, но не лежащую ни на одной из прямых L' и L''. В таком случае $L'+L''=L''+P=P+L'$ является плоскостью и прямые L' и L'' пересекаются в некоторой точке Q. Обозначим теперь через $\varkappa$ проектирование прямой L' из точки P на прямую L'', а через X—некоторую точку прямой L', отличную от Q. Тогда X, P, $X^\varkappa$ будут тремя попарно различными коллинеарными точками, и, следовательно, обычным способом, которым мы неоднократно пользовались выше, можно найти такие элементы b и c, что $P=Fb$, $X=Fc$, $X^\varkappa=F(b+c)$; через a обозначим такой элемент, что $Q=Fa$. Существует такое линейное преобразование τ F-простран-

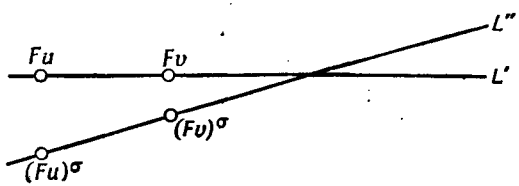
ства A, при котором $a^\tau = a$, $b^\tau = b$, $c^\tau = b + c$ и которое оставляет неподвижным каждый элемент некоторого подпространства, дополнительного к плоскости $L' + L''$. Каждая точка прямой L' имеет вид $F(ua + vc)$. Так как

$$(ua + vc)^\tau = ua + v(b + c) = (ua + vc) + vb,$$

то $[F(ua + vc)]^\tau$ совпадает с пересечением $[F(ua + vc)]^\varkappa$ прямых $L'' = Fa + F(b + c)$ и $F(ua + vc) + P$. Таким образом, проектирование $\varkappa$ индуцируется коллинеацией τ; отсюда и из замечания, сделанного в начале доказательства, следует, что каждое линейное отображение индуцируется коллинеацией.

Пусть теперь отображение σ прямой L' на прямую L'' индуцируется коллинеацией F-пространства A. Поскольку каждая коллинеация индуцируется линейным преобразованием, можно предположить, что σ индуцируется линейным преобразованием η F-пространства A.

Случай 1: $L' \neq L''$ (фиг. 8). Так как на прямой L' расположены по крайней мере три точки, то существуют такие две различные точки Fu и Fv прямой L', образы которых $(Fu)^\sigma = Fu^\eta$



Фиг. 8.

и $(Fv)^\sigma = Fv^\eta$ не принадлежат этой прямой. По крайней мере одна из точек Fu и Fv не лежит на прямой L''; без ограничения общности можно предположить, что на прямой L'' не лежит точка Fv. Если $u^\eta = u'$, $v^\eta = v'$, то из нашего выбора элементов u и v следует, что тройки элементов u, v, u' и v, u', v' линейно независимы. Определим теперь следующим образом линейные преобразования ν и ω соответственно плоскостей $Fu + Fv + Fu'$ и $Fv + Fu' + Fv'$:

$$u^\nu = u',\ v^\nu = v,\ u'^\nu = 2u' - u;\quad v^\omega = v',\ u'^\omega = u',\ v'^\omega = 2v' - v.$$

Легко проверить, что ν индуцирует проектирование прямой $Fu + Fv = L'$ из точки $F(u' - u)$ на прямую $Fu' + Fv$, а ω индуцирует проектирование прямой $Fu' + Fv$ из точки $F(v' - v)$ на прямую $Fu' + Fv' = L''$; также легко проверить, что отображение $\nu\omega$ прямой L' на прямую L'' совпадает с линейным отображением, индуцированным линейным преобразованием η. Таким образом, σ можно представить в виде произведения двух проектирований.

Случай 2: $L' = L''$. Поскольку ранг F-пространства A не меньше 3, в A существует прямая L, отличная от прямой $L' = L''$, но компланарная с ней. Следовательно, существует проектирование σ' прямой L' на прямую L; в первой части доказательства нашего предложения было показано, что σ' индуцируется коллинеацией, а поэтому и линейным преобразованием η' F-пространства A. Так как σ отображает L' на $L'' = L'$, то при отображении $\sigma\sigma'$, индуцированном линейным преобразованием $\eta\eta'$ F-пространства A, образом прямой L' является прямая L. Из приведенных выше рассуждений (случай 1) вытекает, что $\sigma\sigma'$ является произведением двух проектирований. Следовательно, поскольку отображение, обратное проектированию, также представляет собой проектирование, σ будет произведением трех проектирований. Тем самым предложение 7 полностью доказано.

Добавление III

Проективное упорядочение пространства

Пусть нам дано алгебраически упорядоченное тело F. Под этим мы понимаем, что в F выделено определенное подмножество P, называемое *областью положительности* и обладающее следующими свойствами:

(а) P не содержит 0.

(б) Если P содержит x и y, то P содержит $x+y$ и xy.

(в) Если P не содержит $x \neq 0$, то P содержит $-x$.

Числа, принадлежащие P, называются положительными числами. (Читатель может проверить, что если в теле F следующим образом ввести отношение порядка между его элементами: $x < y$ тогда и только тогда, когда $y - x$ содержится в P, то в F будут выполняться все аксиомы упорядоченного тела.)

Легко доказать, что

(г) если $x \neq 0$, то P содержит x^2, а x, x^{-1} оба либо содержатся, либо не содержатся в P.

Доказательство мы оставляем читателю. Из (г) легко следует, что

(д) если P содержит y, то P содержит $x^{-1}yx$ для любого $x \neq 0$ из F.

Рассмотрим теперь четыре попарно различные точки P, Q, R, S, лежащие на прямой L F-пространства A. Их сложное отношение $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}$ является полным классом сопряженных чисел тела F, отличным от 0 и 1. Поэтому, в силу утверждения (д), либо все числа, входящие в данное сложное отношение, принадлежат области положительности P, либо P не содержит ни одного из этих

чисел. В первом случае мы назовем сложное отношение *положительным*, а во втором—*отрицательным*. Введем теперь следующее определение.

Пара точек P, Q тогда и только тогда разделяется парой точек R, S, когда сложное отношение $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}$ *отрицательно и отлично от* 0[1]).

Используя свойства сложного отношения, изложенные нами в замечании 2 (§ 4), читатель легко проверит, что это так называемое циклическое упорядочение точек прямой L удовлетворяет всем аксиомам упорядочения точек проективной прямой[2]). Кроме того, из предложения 7 и леммы 2 (§ 4) следует, что так определенное отношение разделяемости двух пар точек инвариантно относительно всех проектирований и коллинеаций.

Замечание. В то время как теория упорядоченных полей хорошо разработана [теория Артина—Шрейера; см., например, Ван-дер-Варден [2]], о некоммутативных упорядоченных телах пока неизвестно ничего, кроме их существования (см., например, Рейдемейстер [1]) и того, что, как показал Селе [1][3]), понятия упорядоченности и обобщенной формальной действительности эквивалентны.

Другой подход к проблеме упорядочения проективных пространств указан в работах Шпернера [1] и [2].

---

[1]) В оригинале определение было таким: пара точек P, Q тогда и только тогда разделяется парой точек R, S, когда сложное отношение $\begin{bmatrix} P & Q \\ S & R \end{bmatrix}$ положительно и меньше 1. Перед формулировкой определения автор отмечает, что свойство быть меньше (больше) 1 справедливо одновременно для всех чисел, сопряженных с данным числом. Однако, как следует из свойств сложного отношения (см. § 4, замечание 2), при таком определении разделяемости пар точек вместе с парами P, Q и R, S были бы, например, разделены пары S, P и Q, R и не были бы разделены пары P, Q и S, R, что противоречит аксиомам упорядочения точек проективной прямой.—*Прим. перев.*

[2]) Аксиомы упорядочения точек проективной прямой имеются, например, в книге Четверухина Н. Ф. [1], стр. 79.—*Прим. перев.*

[3]) Обобщение результата Селе на случай колец можно найти в работе Поддерюгина В. Д. [1].—*Прим. перев.*

ГЛАВА IV

ДУАЛЬНЫЕ ОТОБРАЖЕНИЯ

В классической проективной геометрии дуальные отображения известны под названием корреляций. Дуальными отображениями являются взаимно однозначные монотонно убывающие соответствия между подпространствами одного и того же или различных линейных многообразий, при которых, в частности, точкам соответствуют гиперплоскости, а гиперплоскостям — точки. В настоящей главе мы найдем алгебраическую интерпретацию дуальных отображений и охарактеризуем те линейные многообразия, между которыми можно установить дуальное соответствие. Алгебраический аппарат, который необходим для этой цели, состоит из так называемых полубилинейных форм, являющихся обобщением таких понятий, как билинейные формы, скалярные произведения, эрмитовы формы и т. д. Более детально мы изучим полярные отображения, т. е. инволюторные автодуальные отображения, являющиеся обобщением классического понятия соответствия между полюсом и его полярой относительно некоторого конического сечения. Группа полярного отображения является обобщением тех так называемых классических групп, которые известны под названием унитарной, симплектической и ортогональной групп; содержание настоящей главы может служить основой для дальнейшего изучения этих групп.

§ 1. Существование дуальных отображений; полубилинейные формы

Дуальным называется такое отображение δ подпространств линейного многообразия (F, A) на подпространства линейного многообразия (G, B), которое обладает следующими свойствами:

(а) δ отображает каждое подпространство T F-пространства A на однозначно определенное подпространство T^δ G-пространства B.

(б) Для каждого подпространства Y G-пространства B существует одно и только одно подпространство X F-пространства A, для которого $X^\delta = Y$.

(в) $U \leqslant V$ тогда и только тогда, когда $V^\delta \leqslant U^\delta$.

Другими словами, дуальным называется взаимно однозначное монотонно убывающее отображение совокупности всех подпро-

странств F-пространства A на совокупность всех подпространств G-пространства B.

В § 3 гл. II мы установили существование дуального соответствия между линейным многообразием конечного ранга и сопряженным ему пространством. Напомним, однако, что сопряженное пространство допускало умножение на элементы основного тела F справа, тогда как исходное пространство допускало умножение на элементы того же тела слева. В настоящей главе мы будем предполагать, что в обоих линейных многообразиях (F, A) и (G, B) имеет место умножение слева на элементы соответствующего основного тела; эта оговорка существенна потому, что бóльшая часть наших исследований относится к случаю, когда $(G, B) = (F, A)$.

Очевидно, что отображение, обратное дуальному, будет дуальным, что произведение двух дуальных отображений, если оно определено, является проективным отображением и что произведение дуального и проективного отображений, если оно определено, будет дуальным отображением. Дуальное отображение линейного многообразия (F, A) самого на себя называется *автодуальным*; линейное многообразие, допускающее автодуальное отображение, называется *двойственным самому себе*. Аналогично, мы будем говорить, что линейные многообразия (F, A) и (G, B) *двойственны друг другу*, если существует дуальное отображение F-пространства A на G-пространство B. Основная цель настоящего параграфа состоит в том, чтобы охарактеризовать двойственные друг другу, в том числе двойственные самим себе, линейные многообразия и найти алгебраическое представление дуальных отображений. Для этого прежде всего отметим несколько простых следствий из определения дуального отображения.

(г) При дуальном отображении образом суммы подпространств является пересечение образов соответствующих подпространств и, наоборот, образом пересечения подпространств является сумма образов соответствующих подпространств.

Это свойство проверяется аналогично свойству (д) проективного отображения (см. гл. III, § 1).

(д) Если δ есть дуальное отображение линейного многообразия (F, A) на линейное многообразие (G, B), то $0^{\delta} = B$, $A^{\delta} = 0$.

Это утверждение непосредственно вытекает из (г).

(е) При дуальном отображении образом точки является гиперплоскость, а образом гиперплоскости — точка.

Утверждение (е) следует из (в) и из того, что не существует подпространства, расположенного строго между 0 и точкой или между гиперплоскостью и всем линейным многообразием.

В силу утверждения (д), дуальные отображения линейных многообразий ранга 1 тривиальны. Подобным же образом из (д) и (е) следует, что любое взаимно однозначное отображение совокупности всех точек одной прямой на совокупность всех точек некоторой

другой прямой можно рассматривать как дуальное отображение первой прямой на вторую. Таким образом, изучение дуальных отображений перестает быть тривиальным только в случае, когда ранги линейных многообразий не меньше 3.

Теорема существования. *Линейное многообразие* (F, A) *тогда и только тогда обладает дуальным отображением, когда его ранг* $r(A)$ *конечен.*

Доказательство этой основной теоремы будет получено в процессе изучения двойственных друг другу линейных многообразий. Для того, чтобы охарактеризовать двойственные друг другу линейные многообразия, нам понадобится следующее понятие.

Инверсно изоморфным отображением тела F *на тело* G называется такое взаимно однозначное отображение α тела F на тело G, при котором

$$(x+y)^\alpha = x^\alpha + y^\alpha \text{ и } (xy)^\alpha = y^\alpha x^\alpha \text{ для любых } x, y \text{ из } F.$$

Если G, в частности, совпадает с F, то α называется инверсным автоморфизмом тела F. Заметим, что каждое изоморфное отображение поля является в то же время инверсно изоморфным отображением и что тождественный автоморфизм тела F тогда и только тогда является инверсным автоморфизмом, когда F есть поле. Примером инверсного автоморфизма некоммутативного тела является уже встречавшееся нам отображение тела действительных кватернионов самого на себя, при котором кватерниону $x_0 + x_1 i + x_2 j + x_3 k$ соответствует «сопряженный» ему кватернион $x_0 - x_1 i - x_2 j - x_3 k$. (Отдельные свойства инверсных автоморфизмов мы рассматривали в § 4 гл. III.)

Теорема о двойственных линейных многообразиях. *Линейные многообразия* (F, A) *и* (G, B), *ранги которых не меньше* 3, *двойственны друг другу тогда и только тогда, когда*

(а) *ранги* $r(A)$, $r(B)$ *конечны и равны между собой и*

(б) *существует инверсно изоморфное отображение тела* F *на тело* G.

Частным случаем этой теоремы, когда $(G, B) = (F, A)$, является

Теорема о двойственном самому себе линейном многообразии. *Линейное многообразие* (F, A), *ранг которого не меньше* 3, *тогда и только тогда двойственно само себе, когда ранг* $r(A)$ *конечен и тело* F *обладает инверсным автоморфизмом.*

Доказательство этих теорем будет следовать из излагаемых ниже результатов, которые интересны и сами по себе.

Лемма 1. *Если* δ *есть дуальное отображение линейного многообразия* (F, A) *на линейное многообразие* (G, B) *и если* X — *подпространство* F-*пространства* A, *то* $r(B/X^\delta) = r[L(X)]$.

Здесь $L(X)$ является сопряженным пространством для линейного многообразия (F, X), введенным и изученным в § 3 гл. II.

Доказательство. Обозначим через K базис сопряженного пространства $L(X)$. Если элемент k принадлежит K, то k является ненулевой линейной формой над X, и $S(k)$ (т. е. совокупность всех таких элементов x из X, что $xk=0$), в силу предложения 3 (а) (гл. II, § 3), будет гиперплоскостью F-пространства X. Покажем, что

(1.1) если $k_0, \ldots, k_n$ – конечное число попарно различных элементов базиса K, то $S(k_1) \cap \ldots \cap S(k_n)$ не содержится в $S(k_0)$.

Действительно, так как K есть базис сопряженного пространства $L(X)$, то ранги подпространств $\sum_{i=1}^{n} k_i F = U$ и $\sum_{i=0}^{n} k_i F = V$ F-пространства $L(X)$ равны соответственно n и $n+1$. Эти ранги конечны; поэтому, используя предложение 3 (а) (гл. II, § 3), мы получаем

$$n = r(U) = r[X/S(U)] < n+1 = r(V) = r[X/S(V)].$$

Таким образом, из $U < V$ следует $S(V) < S(U)$. Далее, легко проверить, что

$$S(V) = S(k_0) \cap S(k_1) \cap \ldots \cap S(k_n) = S(k_0) \cap S(U) < S(U),$$

откуда следует невозможность включения $S(U) \leqslant S(k_0)$, что и требовалось доказать.

(1.2) $\prod_{k \in K} S(k) = 0$.

В самом деле, легко видеть, что рассматриваемое пересечение совпадает с подпространством

$$S\left(\sum_{k \in K} kF\right) = S[L(X)] = S[E(0)] = 0;$$

последнее равенство имеет место в силу предложения 2 (гл. II, § 3),

Теперь для каждого k из K мы положим $k^* = S(k)^\delta$. Так как $S(k)$ – гиперплоскость F-пространства X, то k^*/X^δ является точкой фактор-пространства B/X^δ. Из утверждения (1.2) и свойства (г) дуального отображения вытекает, что B/X^δ является суммой точек вида k^*/X^δ, а из утверждения (1.1) следует, что точки вида k^*/X^δ образуют независимое множество точек фактор-пространства B/X^δ. (Напомним, что множество точек называется независимым, если независимо каждое его конечное подмножество, и что конечное множество точек является независимым, если ни одна из точек этого множества не содержится в сумме остальных.) Таким образом, точки k^*/X^δ образуют базис фактор-пространства

B/X^{δ}[1]). Так как число всех точек вида k^*/X^{δ} совпадает с числом элементов базиса K и так как первое из этих чисел является рангом фактор-пространства B/X^{δ}, а второе — рангом сопряженного пространства $L(X)$, то тем самым показано, что $r(B/X^{\delta}) = r[L(X)]$.

Доказательство конечности ранга. Пусть δ — дуальное отображение линейного многообразия (F, A) на линейное многообразие (G, B). Тогда, полагая в лемме 1 $X = A$ и принимая во внимание, что $A^{\delta} = 0$, мы получаем, что $r(B) = r[L(A)]$. Таким образом, по теореме 1 (гл. II, § 3), $r(A) \leqslant r[L(A)] = r(B)$. Но так как отображение, обратное дуальному, также является дуальным, то подобным же образом можно показать, что

$$r(B) \leqslant r[L(B)] = r(A).$$

Из полученных неравенств следует, что $r(A) = r[L(A)]$; отсюда и из следствия 1 (гл. II, § 3) вытекает конечность ранга $r(A)$.

Следствие 1. *Если δ есть дуальное отображение линейного многообразия (F, A) на линейное многообразие (G, B), то*

$$r(B) = r(X) + r(X^{\delta})$$

для каждого подпространства X F-пространства A.

[Заметим, что в случае, когда $X = A$, выписанное равенство принимает вид $r(B) = r(A)$.]

Доказательство. Выше было показано, что из существования дуального отображения следует конечность рангов линейных многообразий (F, A) и (G, B). Поэтому, используя лемму 1, специальную формулу для ранга (гл. II, § 2) и теорему 1 (гл. II, § 3), мы получаем

$$r(B) - r(X^{\delta}) = r(B/X^{\delta}) = r[L(X)] = r(X),$$

что и требовалось доказать.

ПОСТРОЕНИЕ КАНОНИЧЕСКОГО ДВОЙСТВЕННОГО ПРОСТРАНСТВА

Линейное многообразие (F^*, A^*), которое мы сейчас построим, будет, в случае конечности ранга $r(A)$, двойственным линейному многообразию (F, A). Для того, чтобы построить это так называемое каноническое двойственное пространство, построим сначала тело F^*, инверсно изоморфное телу F. Аддитивная группа тела F^* совпадает с аддитивной группой тела F, а умножение в F^*

[1]) Базис линейного многообразия автором определен как максимальное множество линейно независимых элементов. Однако легко проверить, что это определение базиса эквивалентно определению базиса как максимального независимого множества точек. — *Прим. перев.*

определим с помощью равенства

$$x*y = yx$$

(где yx — произведение в теле F).

Легко видеть, что тождественное отображение является инверсно изоморфным отображением тела F на F^* (отсюда, в частности, следует, что F^* будет телом); этот инверсный изоморфизм тела F на тело F^* мы обозначим через γ.

Теперь построим линейное многообразие (F^*, A^*) следующим образом. В качестве аддитивной группы A^* возьмем аддитивную группу $L(A)$, а умножение элемента x из F^* на элемент f из A^* определим с помощью равенства

$$x*f = fx$$

(где fx — обычное произведение линейной формы f над A на элемент x тела F). Если через γ обозначить тождественное отображение аддитивной группы $L(A)$ (на A^*), то γ будет изоморфным отображением аддитивной группы $L(A)$ на аддитивную группу A^*, удовлетворяющим условию

$$(fx)^\gamma = x^\gamma * f^\gamma \text{ для } f \text{ из } L(A) \text{ и } x \text{ из } F.$$

Очевидно, что это тождественное отображение аддитивной группы $L(A)$ задает отображение, которое естественно назвать инверсно изоморфным отображением линейного многообразия $(L(A), F)$, допускающего умножение на элементы из F справа, на многообразие (F^*, A^*), допускающее умножение на элементы из F^* слева. Отсюда, в частности, следует, что (F^*, A^*) является линейным многообразием. Заметим, наконец, что каждое подпространство X линейного многообразия $(L(A), F)$ является в то же время подпространством линейного многообразия (F^*, A^*), поскольку X и X^γ состоят из одних и тех же элементов. Теперь с помощью теоремы 3 (гл. II, § 3) нетрудно вывести следующее утверждение.

(ж) *Если ранг $r(A)$ конечен, то отображение каждого подпространства X линейного многообразия (F, A) на подпространство $E(X)$ линейного многообразия (F^*, A^*) является дуальным отображением (F, A) на (F^*, A^*).*

Выше было показано, что из существования дуального отображения вытекает конечность ранга отображаемого линейного многообразия. Отсюда и из только что доказанного утверждения следует справедливость сформулированной ранее теоремы существования.

Лемма 2. *Если δ есть дуальное отображение линейного многообразия (F, A) на линейное многообразие (G, B) и если ранг $r(A)$ не меньше 3, то существует такой инверсный изоморфизм σ' тела F на тело G и такой изоморфизм σ'' аддитивной группы A*

на аддитивную группу $L(B)$, *что*

$$(xa)^{\sigma''} = a^{\sigma''} x^{\sigma'} \text{ для } a \text{ из } A \text{ и } x \text{ из } F,$$

$$X^{\sigma''} = E(X^{\delta}) \text{ и } X^{\delta} = S(X^{\sigma''})$$

для каждого подпространства X F-*пространства* A. [Такую пару отображений (σ', σ'') мы будем называть *инверсным полулинейным преобразованием* (см. гл. V, § 5).]

Доказательство. Построим для линейного многообразия (G, B) каноническое двойственное пространство (G^*, B^*) и обозначим одним и тем же символом ρ тождественное отображение G на G^* и тождественное отображение $L(B)$ на B^*. Из существования дуального отображения линейного многообразия (F, A) на линейное многообразие (G, B), в силу теоремы существования и следствия 1, вытекает, что (F, A) и (G, B) имеют равные конечные ранги. Поэтому, отображая подпространство Y G-пространства B на подпространство $E(Y)$ G^*-пространства B^*, мы, в силу утверждения (ж), получаем дуальное отображение (G, B) на (G^*, B^*). Если теперь X есть подпространство F-пространства A, то X можно отобразить на подпространство $E(X^{\delta})$ G^*-пространства B^*; очевидно, что так определенное отображение является проективным (оно представляет собой произведение двух дуальных отображений). Так как, по предположению, $r(A) \geqslant 3$, то, в силу первой основной теоремы проективной геометрии (гл. III, § 1), существует такое полулинейное преобразование σ F-пространства A на G^*-пространство B^*, что $E(X^{\delta}) = X^{\sigma}$ для каждого подпространства X F-пространства A. Изоморфное отображение σ тела F на тело G^* определяет в то же время инверсно изоморфное отображение σ' тела F на тело G (причем $\sigma = \sigma'\rho$), а изоморфное отображение σ группы A на группу B^* — изоморфное отображение σ'' группы A на группу $L(B)$ (причем $\sigma = \sigma''\rho$). В силу предложения 2 (гл. II, § 3), имеет место равенство $Z = S[E(Z)]$ для каждого подпространства Z F-пространства A; используя это равенство, легко завершить доказательство леммы.

Доказательство теоремы о двойственных линейных многообразиях. Необходимость условий (а), (б) непосредственно вытекает из теоремы существования, следствия 1 и леммы 2. Обратно, пусть справедливы условия (а) и (б). Построим каноническое двойственное пространство (G^*, B^*) для линейного многообразия (G, B). Поскольку тела G и G^* инверсно изоморфны, из существования инверсно изоморфного отображения тела F на тело G следует существование изоморфного отображения тела F на тело G^*. Очевидно, что линейные многообразия (G, B) и (G^*, B^*) имеют равные ранги; поэтому и линейные многообразия (F, A) и (G^*, B^*) также имеют равные ранги. Отсюда, в силу структурной теоремы проективной геометрии (гл. III, § 1), следует существование

проективного отображения σ линейного многообразия (F, A) на линейное многообразие (G^*, B^*). В то же время, так как ранг $r(B)$ конечен, то, ввиду (ж), существует дуальное отображение линейного многообразия (G, B) на линейное многообразие (G^*, B^*). Так как отображение, обратное дуальному, также является дуальным, то теперь легко построить дуальное отображение линейного многообразия (F, A) на линейное многообразие (G, B). Таким образом, теорема полностью доказана.

Замечание о принципе двойственности в проективной геометрии. Теорема существования показывает, что теория проективных пространств конечной размерности двойственна сама себе, ибо для каждого конечномерного линейного многообразия (F, A) можно построить двойственное ему линейное многообразие (F^*, A^*), которое (с полным правом, как это видно из его построения) часто называют пространством гиперплоскостей F-пространства A. Таким образом, если линейное многообразие (F, A) обладает некоторым свойством, то линейное многообразие (F^*, A^*) обладает двойственным свойством; если же некоторое свойство справедливо для каждого линейного многообразия (F, A) конечного ранга, то двойственное свойство справедливо для каждого линейного многообразия (F^*, A^*), т. е. оно также является универсальным. Но, вообще говоря, нельзя утверждать, что если в линейном многообразии (F, A) справедливо свойство P, то в нем справедливо и свойство, двойственное P, ибо не каждое даже конечномерное F-пространство A двойственно самому себе. Это легко следует из теоремы о двойственных самим себе линейных многообразиях, если принять во внимание, что не каждое тело обладает инверсным автоморфизмом.

Заметим, что каждую перестановку точек прямой можно рассматривать как автодуальное отображение этой прямой. Следовательно, предыдущие основные теоремы перестают быть справедливыми, если отбросить предположение, что $r(A) > 2$.

Начиная отсюда, мы будем почти исключительно заниматься автодуальными отображениями (т. е. дуальными отображениями F-пространства A на себя).

Следствие 2. *Если δ — автодуальное отображение линейного многообразия (F, A), то следующие свойства подпространства M F-пространства A эквивалентны:*

$$\text{(I)}\quad M \cap M^{\delta} = 0;$$

$$\text{(II)}\quad M + M^{\delta} = A;$$

$$\text{(III)}\quad M \dot{+} M^{\delta} = A.$$

Это утверждение почти непосредственно следует из формул для ранга (а), (б) (гл. II, § 2), если принять во внимание, что,

в силу теоремы существования, ранг $r(A)$ конечен и что, в силу следствия 1, $r(A) = r(M) + r(M^{\perp})$.

Заметим, что подпространства, обладающие свойством (I), называются *неизотропными* относительно автодуального отображения δ.

Используя лемму 2, можно получить алгебраическое представление автодуальных отображений. Для этого введем понятие *полубилинейной формы над линейным многообразием* (F, A). Полубилинейная форма есть функция $f(x, y)$, которая связана с определенным инверсным автоморфизмом α тела F и обладает следующими свойствами:

(Ф.1) $f(x, y)$ для каждой пары элементов x, y из A является однозначно определенным числом тела F;

(Ф.2) $f(a+b, c) = f(a, b) + f(b, c)$, $f(a, b+c) = f(a, b) + f(a, c)$ для любых a, b, c из A;

(Ф.3) $f(tx, y) = tf(x, y)$, $f(x, ty) = f(x, y)\, t^{\alpha}$ для x, y из A и t из F.

Поскольку инверсный автоморфизм α является одним из основных объектов при определении полубилинейной формы, мы будем полубилинейную форму f часто называть *α-формой над A*. Если, в частности, $\alpha = 1$ (что возможно только в случае, когда F есть поле), то f называется билинейной формой.

Примеры. 1. Пусть F — поле действительных чисел и A — пространство всех n-строк $x = (x_1, \ldots, x_n)$ с действительными координатами x_i. В этом случае (F, A) является $(n-1)$-мерным действительным проективным пространством. Обычное скалярное произведение

$$xy = \sum_{i=1}^{n} x_i y_i$$

является билинейной формой над A.

2. Пусть F — поле комплексных чисел и A — пространство всех n-строк $x = (x_1, \ldots, x_n)$ с комплексными координатами x_i. Обозначим через α автоморфизм поля F, отображающий каждое число c из F на сопряженное ему число $\bar{c}$. Эрмитова форма $x\bar{y} = \sum_{i=1}^{n} x_i \bar{y}_i$ является α-формой над A.

3. Пусть F — тело действительных кватернионов и α — инверсный автоморфизм тела F, отображающий действительный кватернион $x = x_0 + x_1 i + x_2 j + x_3 k$ (где x_i — действительные числа) на сопряженный кватернион $\bar{x} = x_0 - x_1 i - x_2 j - x_3 k$. Тогда, если обозначить через A пространство всех n-строк $q = (q_1, \ldots, q_n)$ с координатами q_i из F, то гамильтонова форма $x\bar{y} = \sum_{i=1}^{n} x_i \bar{y}_i$ будет α-формой над A.

Матричное представление полубилинейных форм. Предположим, что $f(x, y)$ есть α-форма над линейным многообразием (F, A) конечного ранга n и что $b_1, \ldots, b_n$ — базис этого линейного многообразия. Пусть $f(b_i, b_j) = a_{ij}$, $x = \sum_{i=1}^{n} x_i b_i$. Тогда из свойств (Ф.1) — (Ф.3) полубилинейной формы легко следует, что

$$f(x, y) = \sum_{i,j} x_i a_{ij} y_j^{\alpha}.$$

Используя матричное обозначение, можно записать эту формулу в виде

$$f(x, y) = (x_1, \ldots, x_n)\,(a_{ij}) \begin{pmatrix} y_1 \\ \cdot \\ \cdot \\ \cdot \\ y_n \end{pmatrix}^{\alpha}.$$

Если элементы $c_1, \ldots, c_n$ образуют другой базис F-пространства A, то $c_i = \sum_{j=1}^{n} b_{ij} b_j$ и, следовательно,

$$f(c_i, c_j) = \sum_{h,k} b_{ih} a_{hk} b_{jk}^{\alpha};$$

этим равенствам также можно придать матричный вид. Мы, однако, в дальнейшем такими матричными представлениями нигде пользоваться не будем.

Если f есть полубилинейная форма над (F, A) и K — подмножество F-пространства A, то совокупность решений x уравнений $f(x, K) = 0$ [т. е. совокупность таких элементов x из A, что $f(x, k) = 0$ для каждого k из K], как легко проверить, является подпространством F-пространства A. Точно так же подпространство F-пространства A образуют все решения y уравнений $f(K, y) = 0$.

Мы будем говорить, что *дуальное отображение* δ *линейного многообразия* (F, A) *на себя представимо полубилинейной формой* $f(x, y)$ *над* (F, A), если X^{δ} для каждого подпространства X F-пространства A совпадает с совокупностью решений x уравнений $f(x, X) = 0$. В символической записи

$$X^{\delta} = (x \in A : f(x, X) = 0).$$

Предложение 1. *Каждое автодуальное отображение линейного многообразия, ранг которого не меньше* 3, *представимо полубилинейной формой.*

Историческая справка. Первое доказательство теоремы такого типа содержалось в работе Биркгофа и Неймана [1]; см. в частности, их добавление I, стр. 837 — 843.

Доказательство. Если δ есть автодуальное отображение линейного многообразия (F, A), то, по лемме 2, существуют такой инверсный автоморфизм α тела F и такое изоморфное отображение σ аддитивной группы A на аддитивную группу $L(A)$, что $(xy)^\sigma = y^\sigma x^\alpha$ для x из F и y из A, $X^\delta = S(X^\sigma)$ для каждого подпространства X F-пространства A.

Если x и y — элементы F-пространства A, то xy^σ есть однозначно определенный элемент тела F, ибо y^σ принадлежит сопряженному пространству $L(A)$ и потому является линейной формой над A. Таким образом, можно определить функцию

$$f(x, y) = xy^\sigma$$

для каждой пары элементов x, y из A. Нетрудно проверить, что $f(x, y)$ является α-формой над A. Если теперь X есть подпространство F-пространства A, то совокупность X^* решений x уравнений $f(x, X) = 0$ совпадает с совокупностью решений x уравнений $xX^\sigma = 0$. Отсюда, вспоминая определение оператора S, мы получаем, что $X^* = S(X^\sigma) = X^\delta$. Таким образом, показано, что автодуальное отображение δ представимо полубилинейной формой f, что и требовалось доказать.

Тривиальный пример полубилинейной формы: $f(x, y) = 0$ для любых x и y — показывает, что не каждая полубилинейная форма представляет дуальное отображение. Поэтому нам нужно охарактеризовать те полубилинейные формы, которые представляют дуальные отображения (так называемые невырожденные полубилинейные формы). Для этого мы используем следующую простую связь между полубилинейными формами над (F, A) и линейными формами над (F, A). Если $f(x, y)$ есть α-форма над линейным многообразием (F, A), то каждому элементу y из A можно сопоставить отображение y^f группы A в тело F, определяемое равенством

$$xy^f = f(x, y) \text{ для каждого } x \text{ из } A.$$

Нетрудно проверить, что y^f, для каждого y из A, является линейной формой над A (т. е. y^f принадлежит $L(A)$);

$$(a+b)^f = a^f + b^f, \quad (ta)^f = a^f t^\alpha \text{ для } a, b \text{ из } A \text{ и } t \text{ из } F.$$

Следовательно, отображение y из A на y^f из $L(A)$ можно назвать *инверсно гомоморфным отображением F-пространства A в сопряженное пространство $L(A)$*. Естественно, что если так установленное отображение будет взаимно однозначным, то оно будет инверсно изоморфным; напомним читателю, что, как мы выше показали, тождественное отображение является инверсно изоморфным отображением линейного многообразия $(L(A), F)$ на линейное многообразие (F^*, A^*).

Предложение 2. *Следующие свойства α-формы $f(x, y)$ над линейным многообразием (F, A) эквивалентны:*

(I) *f представляет автодуальное отображение F-пространства A.*

(II) *Ранг $r(A)$ конечен, и из $f(A, y) = 0$ следует $y = 0$.*

(III) $A^f = L(A)$.

(IV) *Ранг $r(A)$ конечен, и из $f(x, A) = 0$ следует $x = 0$.*

(V) *Отображение элемента a из A на элемент a^f из $L(A)$ является инверсно изоморфным отображением F-пространства A на сопряженное пространство $L(A)$.*

Доказательство. Если α-форма f представляет дуальное отображение, то, в силу теоремы существования, ранг $r(A)$ конечен. Если y — такой элемент из A, что $f(A, y) = 0$, то и $f(A, Fy) = 0$. Поэтому при дуальном отображении, представимом α-формой f, подпространство Fy F-пространства A отображается на A. Но единственным прообразом A при автодуальном отображении является 0; отсюда $Fy = 0$ и, следовательно, $y = 0$. Тем самым показано, что свойство (II) вытекает из свойства (I).

Предположим теперь, что справедливо свойство (II). Тогда отображение элемента a из A на элемент a^f из $L(A)$ будет инверсно изоморфным отображением A в $L(A)$, поскольку из $a^f = 0$ следует, что $f(A, a) = 0$, откуда $a = 0$. Таким образом, мы получаем инверсно изоморфное отображение F-пространства A на подпространство A^f сопряженного пространства $L(A)$; отсюда, в частности, следует (как легко проверить различными способами), что $r(A) = r(A^f)$. Но из конечности ранга $r(A)$ и следствия 1 (гл. II, § 3) вытекает, что $r(A) = r[L(A)]$. Поэтому $L(A)$ и его подпространство A^f имеют один и тот же конечный ранг; отсюда и из формулы для ранга (а) (гл. II, § 2) вытекает, что $L(A) = A^f$. Таким образом, свойство (III) следует из свойства (II).

Пусть теперь справедливо свойство (III). Тогда сопряженное пространство $L(A) = A^f$ будет инверсно гомоморфным образом F-пространства A, так что $r[L(A)] \leqslant r(A)$. Отсюда и из теоремы 1 (гл. II, § 3) (а также из теоретико-множественной теоремы о том, что $\varkappa < c^{\varkappa}$) непосредственно следует конечность ранга $r(A)$. Далее, если $f(x, A) = 0$ для некоторого элемента x из A, то $xL(A) = xA^f = f(x, A) = 0$ и, следовательно, x принадлежит $S[L(A)] = S[E(0)] = 0$; последнее равенство имеет место в силу предложения 2 (гл. II, § 3). Тем самым показано, что из свойства (III) следует свойство (IV).

Пусть справедливо свойство (IV). $S(A^f)$ представляет собой совокупность всех решений x уравнений $0 = xA^f = f(x, A)$; следовательно, в силу свойства (IV), $S(A^f) = 0$. Поскольку ранг $r(A)$ конечен, можно воспользоваться предложением 3 (гл. II, § 3), из которого вытекает, что

$$A^f = E[S(A^f)] = E(0) = L(A).$$

Таким образом, из свойства (IV) следует свойство (III). Обозначим теперь через W совокупность решений w уравнений $f(A, w) = 0$. Подпространство W F-пространства A является ядром инверсно гомоморфного отображения A на $A^f = L(A)$, которое получается при сопоставлении элементу a из A элемента a^f из $L(A)$. Поэтому, принимая во внимание конечность рангов всех рассматриваемых здесь пространств, мы из специальной формулы для ранга (гл. II, § 2), свойства (III), которое нами уже было выведено из свойства (IV), и теоремы 1 (гл. II, § 3) получаем, что

$$r(A) - r(W) = r(A^f) = r[L(A)] = r(A),$$

откуда $r(W) = 0$, т. е. $W = 0$. Этим показано, что из свойства (IV) следует также свойство (II). Но если одновременно справедливы свойства (II) и (III), то справедливо и свойство (V); тем самым показано, что свойство (V) вытекает из свойства (IV).

Предположим, наконец, что справедливо свойство (V). Тогда A и $L(A)$ имеют один и тот же ранг $r(A)$, конечный в силу следствия 1 (гл. II, § 3). Теперь можно воспользоваться теоремой 3 (гл. II, § 3), из которой вытекает, что отображение подпространства N сопряженного пространства $L(A)$ на подпространство $S(N)$ F-пространства A является дуальным отображением $L(A)$ на A. В то же время, в силу свойства (V), отображение подпространства X F-пространства A на подпространство X^f сопряженного пространства $L(A)$ является проективным отображением A на $L(A)$. Вследствие этого, отображая подпространство X F-пространства A на подпространство $S(X^f)$, мы получаем автодуальное отображение σ F-пространства A. Но, по определению, $S(X^f)$ есть совокупность всех элементов x из A, удовлетворяющих уравнениям

$$0 = xX^f = f(x, X);$$

этим показано, что автодуальное отображение σ представимо α-формой f. Таким образом, из свойства (V) следует свойство (I); тем самым предложение 2 полностью доказано.

Замечание. Если B есть базис линейного многообразия (F, A) и α — инверсный автоморфизм тела F, то существует, и притом только одна, такая α-форма $f(x, y)$, что

$$f(b', b'') = \begin{cases} 1 \text{ для } b' = b'' \text{ из } B, \\ 0 \text{ для } b' \neq b'' \text{ из } B. \end{cases}$$

Легко проверить, что f обладает следующими свойствами: из $f(A, x) = 0$ следует $x = 0$ и из $f(a, A) = 0$ следует $a = 0$ независимо от того, конечен ли ранг $r(A)$ или бесконечен. Это показывает, что требование конечности ранга в формулировках свойств (II) и (IV) является необходимым для справедливости предложения 2.

Предположим теперь, что α-форма $f(x, y)$ представляет дуальное отображение линейного многообразия (F, A), и рассмотрим функцию $g(x, y) = f(x, y)d$, где d — отличный от 0 элемент тела F. Из свойства (Ф.3) полулинейной формы следует, что

$$g(x, ty) = f(x, ty)d = f(x, y)t^{\alpha}d = g(x, y)(d^{-1}t^{\alpha}d)$$

для любых x, y из A и t из F. Если положить $t^{\beta} = d^{-1}t^{\alpha}d$, то β будет инверсным автоморфизмом тела F (β является произведением инверсного автоморфизма α на внутренний автоморфизм). Легко проверить, что g будет β-формой над (F, A), представляющей то же самое дуальное отображение δ, что и f. Если w — элемент F-пространства A, не содержащийся в $(Fw)^{\delta}$, то $f(w, w) \neq 0$; полагая поэтому $d^{-1} = f(w, w)$, мы получаем, что новая форма g удовлетворяет условию $g(w, w) = 1$. Нормализацией такого рода мы будем в дальнейшем часто пользоваться.

Предыдущее замечание показывает, что автодуальное отображение определяет представляющие его полулинейные формы не однозначно. Однако, как видно из следующего утверждения, все полулинейные формы, представляющие данное автодуальное отображение, исчерпываются совокупностью полулинейных форм, построенной выше.

Предложение 3. *Если полулинейные формы f и g над (F, A) представляют одно и то же автодуальное отображение F-пространства A и если $r(A) \geqslant 2$, то в F существует такое число $d \neq 0$, что*

$$g(x, y) = f(x, y)d \quad \textit{для любых } x, y \textit{ из } A.$$

Доказательство. Из предложения 2 следует, что отображение элемента a из A на элемент a^f из $L(A)$ является инверсно изоморфным отображением F-пространства A на сопряженное пространство $L(A)$ и что также инверсно изоморфным отображением A на $L(A)$ будет отображение каждого элемента a из A на элемент a^g из $L(A)$. Поэтому существует такое полулинейное преобразование σ сопряженного пространства $L(A)$ на себя, что $(a^f)^{\sigma} = a^g$ для каждого a из A. Если X есть подпространство F-пространства $L(A)$, то существует такое однозначно определенное подпространство T F-пространства A, что $X = T^f$. Автодуальные отображения, представимые полулинейными формами f и g, отображают T соответственно на $S(T^f)$ и $S(T^g)$; так как f и g представляют одно и то же автодуальное отображение, то $S(T^f) = S(T^g)$. Теперь, поскольку существование дуального отображения предполагает конечность ранга $r(A)$, мы воспользуемся предложением 3 (гл. II, § 3), из которого следует, что

$$T^f = E[S(T^f)] = E[S(T^g)] = T^g.$$

Отсюда вытекают равенства

$$X^{\sigma} = T^{f\sigma} = T^{g} = T^{f} = X.$$

Но так как, согласно предположению, $r(A) \geqslant 2$, то можно воспользоваться предложением 3 (гл. III, § 1), в силу которого лишь тривиальные полулинейные преобразования оставляют инвариантным каждое подпространство. Таким образом, σ является тривиальным полулинейным преобразованием, а это означает, что в теле F существует такое число $d \neq 0$, что $z^{\sigma} = zd$ для каждого z из $L(A)$. Поэтому

$$g(x, y) = xy^{g} = xy^{f\sigma} = xy^{f}d = f(x, y)\,d,$$

что и требовалось доказать.

§ 2. Нуль-системы [1])

Нуль-системы представляют собой довольно частный класс автодуальных отображений. Однако результаты этого параграфа будут существенно использованы в следующем параграфе.

Автодуальное отображение δ линейного многообразия (F, A) называется *нуль-системой на подпространстве* W F-пространства A, а W называется *N-подпространством* F-пространства A относительно δ, если

$$P \leqslant P^{\delta} \text{ для каждой точки } P \text{ подпространства } W. \qquad (N)$$

Автодуальное отображение, являющееся нуль-системой на всем A, называется нуль-системой линейного многообразия (F, A).

Лемма 1. *Если α-форма f представляет дуальное отображение δ линейного многообразия (F, A), то:*

(а) *δ тогда и только тогда будет нуль-системой на подпространстве W, когда $f(x, x) = 0$ для каждого x из W.*

(б) *Если δ является нуль-системой на W, то $f(x, y) = -f(y, x)$ для любых x, y из W.*

(в) *Если δ является нуль-системой на W и $f(W, W) \neq 0$, то $\alpha = 1$, так что F будет полем.*

Доказательство. Так как автодуальное отображение δ представимо α-формой f, то элемент a из A тогда и только тогда содержится в X^{δ}, где X — подпространство F-пространства A, когда $f(a, X) = 0$. Поэтому $Fx \leqslant (Fx)^{\delta}$ тогда и только тогда, когда $f(x, x) = 0$; из этого замечания непосредственно следует справедливость утверждения (а).

Если N-подпространство W содержит элементы x и y, то в W содержится и их сумма $x + y$; отсюда, используя утверждение (а),

[1]) В книге Ходжа и Пидо [1] вместо термина «нуль-система» употребляется термин «нуль-полярная корреляция».—*Прим. перев.*

мы получаем

$$0 = f(x+y, x+y) = f(x, x) + f(y, x) + f(x, y) + f(y, y) = \\ = f(x, y) + f(y, x),$$

что и доказывает справедливость утверждения (б). Если, кроме того, $f(W, W) \neq 0$, то в W найдутся такие элементы v и w, что $t = f(v, w) \neq 0$. Используя теперь утверждение (б), мы для любого x из F получаем

$$xt = xf(v, w) = f(xv, w) = -f(w, xv) = -f(w, v)\, x^\alpha = f(v, w)\, x^\alpha = tx^\alpha.$$

Таким образом, $x^\alpha = t^{-1}xt$ для каждого x из F; тем самым показано, что инверсный автоморфизм α совпадает с внутренним автоморфизмом, индуцированным элементом t. Но инверсный автоморфизм тогда и только тогда является автоморфизмом, когда F есть поле; единственным же внутренним автоморфизмом поля является тождественный автоморфизм. Таким образом, $\alpha = 1$ и F — поле, что и требовалось доказать.

Лемма 2. *Если дуальное отображение δ представимо полубилинейной формой f и если W — такое N-подпространство, что $f(W, W) \neq 0$, то:*

(а) *W содержит такие элементы x, y, что $f(x, y) = 1$.*

(б) *Если P и Q — точки подпространства W, причем точка P не принадлежит гиперплоскости Q^δ, то $P+Q=L$ будет такой прямой, что $L \cap L^\delta = 0$.*

Доказательство. Поскольку $f(W, W) \neq 0$, в W существуют такие элементы u', v, что $t = f(u', v) \neq 0$. Полагая $u = t^{-1}u'$, мы получаем $f(u, v) = 1$. Если точки $P = Fp$ и $Q = Fq$ принадлежат подпространству W, то, по лемме 1 (а), $f(p, p) = f(q, q) = 0$. Если точка P не лежит на гиперплоскости Q^δ, то, поскольку W является N-подпространством, $P \neq Q$ и $f(p, q) \neq 0$. Из леммы 1 (б) вытекает, что и $f(q, p) = -f(p, q) \neq 0$. Если теперь элемент w принадлежит пересечению $L \cap L^\delta$, где $L = P+Q$, то $w = hp + kq$ и $f(w, L) = 0$, так что

$$0 = f(w, p) = kf(q, p), \text{ откуда } k = 0,$$
$$0 = f(w, q) = hf(p, q), \text{ откуда } h = 0.$$

Таким образом, $w = 0$ и, следовательно, $L \cap L^\delta = 0$.

Замечание 1. Если дуальное отображение δ представимо полубилинейной формой f, то следующие свойства подпространства W F-пространства A эквивалентны: W не содержится в W^δ; $W \cap W^\delta < W$; $f(W, W) \neq 0$. Эти свойства, в частности, справедливы для неизотропного подпространства $W \neq 0$ (т. е. подпространства, удовлетворяющего условию $W \cap W^\delta = 0$; см. стр. 130).

Предложение 1. *Если дуальное отображение δ представимо α-формой f, то подпространство $W \neq 0$ тогда и только тогда является неизотропным N-подпространством, когда $\alpha = 1$, $r(W) = 2k$ и в W существует такой базис $b_1, \ldots, b_{2k}$, что $f(b_{2i-1}, b_{2i}) = -f(b_{2i}, b_{2i-1}) = 1$ и $f(b_i, b_j) = 0$ в остальных случаях.*

Доказательство. Предположим сначала, что $\alpha = 1$ (следовательно, F есть поле) и что в W существует базис $b_1, \ldots, b_{2k}$, обладающий указанным в формулировке предложения свойством. Тогда

$$f\left(\sum_{i=1}^{2k} x_i b_i, \sum_{i=1}^{2k} y_i b_i\right) = \sum_{i=1}^{k} [x_{2i-1}y_{2i} - x_{2i}y_{2i-1}]. \qquad (1^*)$$

Используя эту формулу, можно простым подсчетом проверить, что $f(w, w) = 0$ для каждого w из W и $W \cap W^\delta = 0$; таким образом, W будет неизотропным N-подпространством F-пространства A.

Обратно, если W — отличное от 0 неизотропное N-подпространство, то $f(W, W) \neq 0$. Отсюда и из леммы 1 (в) вытекает, что $\alpha = 1$ и F является полем. В силу леммы 2 (а), в W существуют такие элементы b_1, b_2, что $f(b_1, b_2) = 1$ и, следовательно, по лемме 1 (б), $f(b_2, b_1) = -1$. Поэтому мы можем воспользоваться леммой 2 (б), в силу которой $L = Fb_1 + Fb_2$ будет такой прямой, лежащей в подпространстве W, что $L \cap L^\delta = 0$. Отсюда и из следствия 2 (§ 1) вытекает, что $A = L \dotplus L^\delta$ и, поскольку $L \leqslant W$, $W = L \dotplus (W \cap L^\delta)$. Пусть $V = W \cap L^\delta$. Тогда из общей формулы для ранга (гл. II, § 2) мы получим, что $r(W) = r(L) + r(V) = 2 + r(V)$. Так как подпространство V содержится в N-подпространстве W, то оно само обладает свойством (N). Далее, пользуясь тем, что при дуальном отображении пересечение подпространств отображается на сумму образов этих подпространств, и учитывая неизотропность подпространства W, мы получаем

$$V \cap V^\delta = W \cap L^\delta \cap V^\delta = W \cap (L + V)^\delta = W \cap W^\delta = 0.$$

Таким образом, V является таким неизотропным N-подпространством меньшего чем $r(W)$ ранга, что $0 = f(V, L) = f(L, V)$ [последнее равенство имеет место в силу леммы 1 (б)] и $W = L \dotplus V$. Теперь необходимость условий нашего предложения устанавливается при помощи очевидной индукции, поскольку существование дуального отображения предполагает конечность ранга F-пространства A.

Теорема. *F-пространство A, ранг которого не меньше 3, тогда и только тогда обладает нуль-системой, когда F — поле и $r(A)$ — конечное четное число. Эта нуль-система определяется по существу однозначно.*

Доказательство. Пусть дуальное отображение δ линейного многообразия (F, A) является нуль-системой. В силу предложения 1 (§ 1), δ представимо полубилинейной формой $f(x, y)$.

Поскольку F-пространство A обладает свойством (N) и $f(A, A) \neq 0$, то, по лемме 1, F будет полем, а f — кососимметрической билинейной формой; Так как $A^\delta = 0$, то A является неизотропным N-подпространством; отсюда и из предложения 1 вытекает, что F-пространсиво A имеет конечный и четный ранг. Этим доказана необходимость наших условий; из представления кососимметрической билинейной формы f в виде (1*) следует, что f, а вместе с ней и нуль-система δ определяются по существу однозначно.

Обратно, если F-пространство A удовлетворяет условиям теоремы, то по формуле (1*) можно определить кососимметрическую билинейную форму над (F, A), которая, как легко проверить, будет представлять нуль-систему.

Замечание 2. Дуальное отображение произвольной прямой (F, A), отображающее каждую точку на себя, является нуль-системой; следовательно, в этом случае условия нашей теоремы не являются необходимыми. Подобного рода замечание можно сделать и относительно случая, когда (F, A) является точкой.

Предложение 2. *Если дуальное отображение δ представимо полулинейной формой f над (F, A) и если W является N-подпространством F-пространства A, то следующие свойства подпространства M, содержащегося в W, эквивалентны:*

(I) $W = M \dotplus (W \cap W^\delta)$.

(II) $r(W) = r(M) + r(W \cap W^\delta)$ *и* $M \cap M^\delta = 0$.

(III) *M является максимальным подпространством, содержащимся в W и удовлетворяющим условию* $M \cap M^\delta = 0$.

Доказательство. Пусть справедливо свойство (I). Тогда, поскольку из существования дуального отображения следует конечность ранга линейного многообразия, мы можем воспользоваться формулой для ранга (б) (гл. II, § 2), в силу которой

$$r(W) = r(M) + r(W \cap W^\delta).$$

Далее, по лемме 1 (б), $f(x, y) = -f(y, x)$ для любых x, y из W. Так как $M \leqslant W$, то $W^\delta \leqslant M^\delta$, и поэтому

$$f(M \cap M^\delta, W \cap W^\delta) = -f(W \cap W^\delta, M \cap M^\delta) \leqslant f(W^\delta, M) = 0.$$

Отсюда вытекает, что

$$f(M \cap M^\delta, W) \leqslant f(M \cap M^\delta, M) + f(M \cap M^\delta, W \cap W^\delta) \leqslant$$
$$\leqslant f(M^\delta, M) = 0.$$

Таким образом, $M \cap M^\delta \leqslant W^\delta$ и, следовательно, $M \cap M^\delta \leqslant$ $\leqslant M \cap W \cap W^\delta = 0$. Тем самым показано, что при выполнении свойства (I) выполняется и свойство (II).

Предположим теперь, что M обладает свойством (II) и что подпространство N удовлетворяет условиям $M \leqslant N \leqslant W$ и $N \cap N^\delta = 0$. Тогда $W^\delta \leqslant N^\delta$, и поэтому $N \cap (W \cap W^\delta) = N \cap W^\delta \leqslant N \cap N^\delta = 0$. Теперь из свойства (II) и формулы для ранга (б) (гл. II, § 2) вытекает, что

$$r(W) = r(M) + r(W \cap W^\delta) \leqslant r(N) + r(W \cap W^\delta) = \\ = r(N + [W \cap W^\delta]) \leqslant r(W).$$

Отсюда $r(N) = r(M)$, и, следовательно, $N = M$, чем доказана максимальность подпространства M. Таким образом, из свойства (II) следует свойство (III).

Пусть, наконец, выполняется свойство (III). Так как $M \cap M^\delta = 0$, то в силу следствия 2 (§ 1), $A = M \dot{+} M^\delta$; отсюда и из включения $M \leqslant W$ вытекает, что $W = M \dot{+} (W \cap M^\delta)$. Из $M \leqslant W$ следует также, что $W^\delta \leqslant M^\delta$, и поэтому $W \cap W^\delta \leqslant W \cap M^\delta$. В силу принципа дополнения (гл. II, § 1), существует такое подпространство T, что $W \cap M^\delta = T \dot{+} (W \cap W^\delta)$ и, следовательно, $W = N \dot{+} (W \cap W^\delta)$, где $N = M \dot{+} T$. Но в таком случае, поскольку, как было уже показано, из условия (I) следует условие (II), $N \cap N^\delta = 0$. Отсюда, а также из включения $M \leqslant N$ и максимальности подпространства M вытекает, что $M = N$ и, следовательно, $W = M \dot{+} (W \cap W^\delta)$. Тем самым показано, что если выполняется свойство (III), то выполняется и свойство (I).

Замечание 3. Очевидно, что всегда существует подпространство M, удовлетворяющее условию (I). Таким образом, в силу предложения 2 всегда существует прямое разложение N-подпространства W на неизотропную компоненту M и однозначно определенную компоненту $W \cap W^\delta$. Легко видеть, что $W \cap W^\delta$ удовлетворяет условию

$$f(W \cap W^\delta, W \cap W^\delta) \leqslant f(W^\delta, W) = 0,$$

которое означает, что $W \cap W^\delta \leqslant (W \cap W^\delta)^\delta$. Такое подпространство называется строго изотропным (см. в связи с этим ниже лемму 2, § 4).

§ 3. Представление полярных отображений

Автодуальное отображение σ линейного многообразия (F, A) (в этом параграфе всюду предполагается, что ранг линейного многообразия не меньше 3) называется *полярным отображением*, если $\sigma^2 = 1$. Так как для полярного отображения σ равенство $X^\sigma = Y$ справедливо тогда и только тогда, когда $Y^\sigma = X$, то поляр-

ное отображение σ разбивает все подпространства F-пространства A на пары. Если, в частности, такая пара образована из P и H, где $P = H^\sigma$ является точкой, а $H = P^\sigma$ [в силу свойства (е) дуальных отображений, § 1] — гиперплоскостью, то P называется *полюсом* гиперплоскости H, а H *полярой* точки P. Читатель видит, конечно, что наше понятие полярного отображения является прямым обобщением «полярного соответствия относительно конического сечения», при котором прямой соответствует точка, и наоборот. Основная симметрия полярного отображения σ выражается следующими формулами:

$$X \cap X^\sigma = (X + X^\sigma)^\sigma, \quad X + X^\sigma = (X \cap X^\sigma)^\sigma$$

для каждого подпространства X F-пространства A.

Лемма 1. *Если дуальное отображение σ представимо полубилинейной формой $f(x, y)$, то σ тогда и только тогда будет полярным отображением, когда*

$$\text{из } f(x, y) = 0 \text{ следует } f(y, x) = 0. \qquad (S)$$

Доказательство. Если σ — полярное отображение и $f(x, y) = 0$, то, поскольку f представляет σ, $Fx \leqslant (Fy)^\sigma$ и, следовательно, $Fy \leqslant (Fx)^\sigma$, так что $f(y, x) = 0$. Этим необходимость условия (S) доказана.

Обратно, пусть выполняется условие (S). Так как полубилинейная форма f представляет дуальное отображение σ, то $f(X^\sigma, X) = 0$ для каждого подпространства X F-пространства A. Отсюда и из условия (S) вытекает, что $f(X, X^\sigma) = 0$, и поэтому $X \leqslant X^{\sigma^2}$. В силу следствия 1 (§ 1), $r(A) = r(X) + r(X^\sigma) = r(X^\sigma) + r(X^{\sigma^2})$. Таким образом, $r(X) = r(X^{\sigma^2})$, и теперь равенство $X = X^{\sigma^2}$ вытекает из включения $X \leqslant X^{\sigma^2}$ и формулы для ранга (а) (гл. II, § 2), которой мы можем воспользоваться ввиду конечности ранга F-пространства A (см. теорему существования, § 1). Следовательно, $\sigma^2 = 1$, т. е. σ является полярным отображением.

Следствие 1. *Нуль-системы являются полярными отображениями.*

Это утверждение непосредственно следует из леммы 1 и леммы 1 (б) (§ 2).

Предложение 1. *Если α-форма f представляет полярное отображение σ и если $f(w, w) = 1$ для некоторого элемента w F-пространства A, то $\alpha^2 = 1$ и $f(x, y)^\alpha = f(y, x)$ для любых x, y из A.*

Доказательство. Пусть $H = (Fw)^\sigma$. Тогда, поскольку Fw является точкой, H будет гиперплоскостью. Так как $f(H, w) = 0$, то элемент w не может содержаться в H. Следовательно, $H \cap Fw = 0$; отсюда и из следствия 2 (§ 1) вытекает, что $A = Fw + H$. Покажем теперь, что справедливы следующие утверждения:

(1.1) Если u, v — элементы из H и s, t — такие числа из F, что $st^\alpha = f(u, v)$, то $ts^\alpha = f(v, u)$.

Действительно, так как элементы u, v содержатся в $H = (Fw)^\sigma$, то $0 = f(u, w) = f(v, w)$; отсюда и из условия (S) леммы 1 следует, что $0 = f(w, u) = f(w, v)$. Поэтому, если $st^\alpha = f(u, v)$, то

$$f(sw + u, tw - v) = sf(w, w)t^\alpha + f(u, w)t^\alpha - sf(w, v) - f(u, v) = 0,$$

и, вновь используя условие (S) леммы 1, мы получаем

$$0 = f(tw - v, sw + u) = ts^\alpha - f(v, u);$$

тем самым утверждение (1.1) доказано.

(1.2) Если u, v — элементы из H, то $f(u, v)^\alpha = f(v, u)$.

Это утверждение непосредственно следует из утверждения (1.1), ибо, полагая $t = 1$ и $s = f(u, v)$, мы получаем $f(v, u) = ts^\alpha = f(u, v)^\alpha$, что и требовалось доказать.

(1.3) $\alpha^2 = 1$.

Для того чтобы доказать это утверждение, прежде всего заметим, что $H \neq 0$ и поэтому, в силу предложения 2 (§ 1),

$$0 \neq f(H, A) = f(H, Fw \dotplus H) = f(H, H);$$

последнее равенство имеет место ввиду того, что $f(H, Fw) = 0$, так как $H = (Fw)^\sigma$. Следовательно, в H можно найти такие элементы h и k, что $f(h, k) = 1$. Если теперь t — отличный от 0 элемент тела F, то и $t^\alpha \neq 0$; поэтому в F существует один и только один элемент s такой, что $st^\alpha = 1$. Таким образом, $st^\alpha = f(h, k)$ и, в силу утверждения (1.1), $ts^\alpha = f(k, h)$. Но из утверждения (1.2) следует, что $1 = f(h, k)^\alpha = f(k, h)$. Поэтому $ts^\alpha = 1$. С другой стороны, так как α есть инверсный автоморфизм тела F, то

$$1 = (st^\alpha)^\alpha = t^{\alpha^2}s^\alpha.$$

Таким образом, $t^{\alpha^2} = (s^\alpha)^{-1} = t$, откуда $\alpha^2 = 1$.

Если x, y — элементы F-пространства A, то, поскольку $A = Fw \dotplus H$, $x = x'w + x''$, $y = y'w + y''$, где $x', y' \in F$ и $x'', y'' \in H$. Принимая теперь во внимание, что

$$0 = f(x'', w) = f(w, x'') = f(y'', w) = f(w, y''),$$

а также используя утверждения (1.2) и (1.3), мы получаем, что

$$f(x, y)^\alpha = [x'y'^\alpha + f(x'', y'')]^\alpha = y'x'^\alpha + f(y'', x'') = f(y, x);$$

тем самым наше предложение полностью доказано.

Если α-форма $f(x, y)$ удовлетворяет условию $f(x, y)^\alpha = f(y, x)$, то мы будем говорить, что f является *α-симметрической формой* или, короче, что f является симметрической формой. Заметим, что все три полубилинейные формы, которые мы привели в качестве при-

меров в § 1, были как раз такого типа. Заметим, кроме того, что инверсный автоморфизм тела F обычно называется *инволюторным инверсным автоморфизмом*, если его квадрат равен 1 (как в предложении 1).

Теорема 1. *Если σ — автодуальное отображение линейного многообразия (F, A) и $r(A) \geqslant 3$, то σ тогда и только тогда будет полярным отображением, когда либо σ является нуль-системой (так что F — поле и σ представимо кососимметрической билинейной формой), либо σ можно представить симметрической α-формой, где α — инволюторный инверсный автоморфизм тела F.*

Доказательство. В силу теоремы § 2, можно предположить, что σ не является нуль-системой; по предложению 1 (§ 1), σ представимо некоторой α-формой $f(x, y)$. Так как σ не является нуль-системой, то в A существует такой элемент w, что $f(w, w) \neq 0$; без ограничения общности можно предположить, что $f(w, w) = 1$ (см. метод нормализации, предложение 3, § 1). Если теперь σ является полярным отображением, то из предложения 1 следует, что α будет инволюторным инверсным автоморфизмом и f — симметрической формой. Обратно, если f — симметрическая форма, то она удовлетворяет условию (S) леммы 1 и, следовательно, σ является полярным отображением.

Теорема 2. *Линейное многообразие (F, A), ранг которого не меньше 3, тогда и только тогда обладает полярным отображением, когда ранг $r(A)$ конечен и тело F обладает инволюторным инверсным автоморфизмом.*

Доказательство. Необходимость наших условий следует из теоремы существования § 1 и предыдущей теоремы 1 (заметим, что $\alpha = 1$ является инволюторным инверсным автоморфизмом[1])). Обратно, если ранг $r(A) = n$ конечен и α — инволюторный инверсный автоморфизм тела F, то обозначим через $b_1, \ldots, b_n$ некоторый базис F-пространства A, а через f — однозначно определенную α-форму над A, удовлетворяющую условиям

$$f(b_i, b_j) = \begin{cases} 1 & \text{для } i = j, \\ 0 & \text{для } i \neq j. \end{cases}$$

Так как $(st^\alpha)^\alpha = ts^\alpha$ для любых s, t из F, то f является симметрической α-формой. Из предложения 2 (§ 1) и теоремы 1 вытекает, что f представляет полярное отображение σ; таким образом, теорема 2 полностью доказана.

Подробное изучение инволюторных инверсных автоморфизмов тел читатель может найти в книге Алберта [2].

Если f является симметрической α-формой над линейным многообразием (F, A), удовлетворяющей условию $f(A, A) \neq 0$, то в A

[1]) Если F — поле. — *Прим. перев.*

можно найти такие элементы u, v, что $f(u, v) = 1$. Из симметричности α-формы f вытекает, что $f(v, u) = 1$ и

$$s = sf(v, u) = f(sv, u) = f(u, sv)^{\alpha} = s^{\alpha^2} \text{ для каждого } s \text{ из } F.$$

Таким образом, свойство $\alpha^2 = 1$ следует из симметричности α-формы f. Это замечание показывает, что при рассмотрении нетривиальной α-симметрической формы f дополнительное предположение о том, что инверсный авторморфизм α является инволюторным, излишне.

§ 4. Подпространства, изотропные и неизотропные относительно полярного отображения; индекс и дефект

Подпространство X линейного многообразия (F, A) [ранг $r(A)$ которого не меньше 2] называется неизотропным относительно данного полярного отображения σ F-пространства A, если $X \cap X^{\sigma} = 0$. Из следствия 2 (§ 1) вытекает, что это требование эквивалентно условию $A = X + X^{\sigma}$, или $A = X \dotplus X^{\sigma}$. Поскольку $X = (X^{\sigma})^{\sigma}$, одновременно с X неизотропно и подпространство X^{σ}; таким образом, каждое неизотропное подпространство определяет разложение линейного многообразия в прямую сумму неизотропных компонент (в связи с этим см. ниже § 6).

Лемма 1. *Если σ — полярное отображение линейного многообразия (F, A) и M — неизотропное подпространство F-пространства A, то отображение σ', определенное на линейном многообразии (F, M) равенством*

$$U^{\sigma'} = M \cap U^{\sigma}$$

для каждого подпространства U F-пространства M, будет полярным.

σ' мы будем называть *полярным отображением, индуцируемым в M полярным отображением* σ, причем в подобных случаях всегда будем подразумевать, что подпространство M неизотропно, ибо иначе σ' может не быть полярным отображением.

Доказательство. Очевидно, что σ' является однозначным отображением подпространств F-пространства M на подпространства того же пространства и что из $U \leqslant V \leqslant M$ следует $V^{\sigma'} \leqslant U^{\sigma'}$ [$\leqslant M$]. Из условий $U \leqslant M$, $\sigma^2 = 1$, $M \cap M^{\sigma} = 0$ и закона Дедекинда мы, наконец, получаем, что

$$U^{\sigma'^2} = M \cap (M \cap U^{\sigma})^{\sigma} = M \cap (M^{\sigma} + U) = U + (M \cap M^{\sigma}) = U,$$

откуда $\sigma'^2 = 1$. Этим показано, что σ' является полярным отображением.

Подпространство X естественно назвать *изотропным*, если оно не является неизотропным; это эквивалентно любому из следующих условий: $X \cap X^\sigma \neq 0$, $X + X^\sigma \neq A$. Очевидно, что подпространство X^σ изотропно тогда и только тогда, когда изотропно подпространство X.

Подпространство $X \neq 0$, удовлетворяющее условию $X \leqslant X^\sigma$, безусловно изотропно; такое подпространство мы будем называть *строго изотропным*. Представляется целесообразным включить в число строго изотропных подпространств и нулевое подпространство. В частности, каждая точка либо неизотропна, либо строго изотропна. Следующее утверждение показывает, что каждое подпространство разлагается в прямую сумму неизотропного и строго изотропного подпространств.

Лемма 2. *Если X и Y — такие подпространства F-пространства A, что $X = Y \dot{+} (X \cap X^\sigma)$, то подпространство $X \cap X^\sigma$ строго изотропно, а Y является максимальным неизотропным подпространством, содержащимся в X.*

Доказательство. Так как

$$X \cap X^\sigma \leqslant X + X^\sigma = (X \cap X^\sigma)^\sigma,$$

то подпространство $X \cap X^\sigma$ строго изотропно. Далее, из $Y \leqslant X$ следует $X^\sigma \leqslant Y^\sigma$; используя теперь закон Дедекинда, мы получаем, что

$$X^\sigma = [Y + (X \cap X^\sigma)]^\sigma = Y^\sigma \cap (X^\sigma + X) = X^\sigma + (Y^\sigma \cap X),$$

т. е. $Y^\sigma \cap X \leqslant X^\sigma$. Следовательно,

$$Y \cap Y^\sigma = X \cap Y \cap Y^\sigma = Y \cap X \cap Y^\sigma \cap X^\sigma = Y^\sigma \cap (Y \cap X \cap X^\sigma) = 0,$$

так как X является прямой суммой подпространств Y и $X \cap X^\sigma$. Этим показано, что подпространство Y неизотропно. Допустим, наконец, что Z — неизотропное подпространство, расположенное между Y и X. В таком случае $X^\sigma \leqslant Z^\sigma$, так что

$$X \cap X^\sigma \cap Z = X^\sigma \cap Z \leqslant Z^\sigma \cap Z = 0,$$

и потому

$$Z = Y \dot{+} (Z \cap X \cap X^\sigma) = Y,$$

что и требовалось доказать.

Читателю следует сравнить этот результат с предложением 2 и замечанием 3 (§ 2).

Следствие 1. *Каждая прямая, обладающая свойством (N)* (см. § 2), *либо неизотропна, либо строго изотропна.*

Доказательство. Из леммы 2 следует, что прямая $L = K \dot{+} (L \cap L^\sigma)$, где K — неизотропное и $L \cap L^\sigma$ — строго изотропное

подпространства. Если бы L не являлась ни неизотропным, ни строго изотропным подпространством, то K и $L \cap L^\sigma$ были бы точками, лежащими на прямой L. Но в таком случае из равенства $K \cap K^\sigma = 0$ следует, что точка K не принадлежит своей поляре K^σ, и поэтому прямая L не обладает свойством (N).

Если P — точка строго изотропного подпространства U F-пространства A, то

$$P \leqslant U \leqslant U^\sigma \leqslant P^\sigma.$$

Отсюда следует, что *каждое строго изотропное подпространство обладает свойством* (N). Обратное утверждение, вообще говоря, неверно, поскольку каждое подпространство обладает свойством (N), если σ является нуль-системой. Но это «почти» единственное исключение, как видно из следующих утверждений.

Предложение 1. *Линейное многообразие* (F, A) *тогда и только тогда обладает полярным отображением* σ, *которое не является нуль-системой, но относительно которого в* A *существует не строго изотропное* N*-подпространство, когда* F *— поле характеристики* 2, *а ранг* $r(A)$ *конечен и не меньше* 3. *Такое полярное отображение* σ *представимо симметрической билинейной формой.*

Доказательство. Предположим сначала, что σ — полярное отображение линейного многообразия (F, A), не являющееся нуль-системой, и что W — не строго изотропное N-подпространство F-пространства A. Тогда в W содержится такое подпространство V, что $W = V \dotplus (W \cap W^\sigma)$; по лемме 2, подпространство V неизотропно, а подпространство $W \cap W^\sigma$ строго изотропно. Поскольку W не строго изотропно, V отлично от 0; так как W является N-подпространством, то и V будет N-подпространством F-пространства A. Неизотропное подпространство V не может быть точкой, ибо в противном случае, обладая свойством (N), оно принадлежало бы своей поляре V^σ; таким образом, $r(V) > 1$. Кроме того, V не может совпасть со всем A, так как тогда само A обладало бы свойством (N) и, следовательно, σ было бы нуль-системой. Тем самым показано, что $r(A) \geqslant 3$; конечность ранга $r(A)$ вытекает из теоремы существования (§ 1). Таким образом, в силу теоремы 1 (§ 3), полярное отображение σ, не являющееся нуль-системой, представимо симметрической α-полубилинейной формой f. Так как $V \neq 0$ является неизотропным N-подпространством F-пространства A, то, в силу предложения 1 (§ 2), V имеет четный ранг, $\alpha = 1$, и, следовательно, F является полем, а f — симметрической билинейной формой. Ввиду неизотропности подпространства V, $f(V, V) \neq 0$; поэтому в V существуют такие элементы u, v, что $f(u, v) \neq 0$. Теперь, воспользовавшись леммой 1 (б) (§ 2) и симметричностью

формы f, мы получаем, что

$$-f(u, v)=f(v, u)=f(u, v), \text{ откуда } 1=-1.$$

Таким образом, характеристика поля F равна 2.

Пусть теперь F будет полем характеристики 2, и пусть ранг линейного многообразия (F, A) равен конечному числу n, не меньшему 3. Через $b_1, \ldots, b_n$ обозначим базис F-пространства A и рассмотрим форму

$$f(\sum_{i=1}^{n} x_i b_i, \sum_{i=1}^{n} y_i b_i)=\sum_{i=1}^{n} x_i y_i. \qquad (*)$$

Очевидно, что f есть симметрическая билинейная форма, представляющая некоторое полярное отображение σ (см. предложение 2, § 1, и лемму 1, § 3). Далее, из свойств поля характеристики 2 следует, что $(x+y)^2=x^2+y^2$ для любых x, y из F; поэтому

$$f(\sum_{i=1}^{n} x_i b_i, \sum_{i=1}^{n} x_i b_i)=[\sum_{i=1}^{n} x_i]^2. \qquad (**)$$

Обозначим теперь через W совокупность всех таких элементов $\sum_{i=1}^{n} x_i b_i$, что $\sum_{i=1}^{n} x_i=0$. Легко проверить, что W является подпространством F-пространства A, а именно гиперплоскостью (см. замечание 2, гл. II, § 3), и что W, в силу формулы (**), обладает свойством (N). Поскольку $1+1=0$ и $n\geqslant 3$, в W содержатся элементы b_1+b_2 и b_2+b_3, для которых $f(b_1+b_2, b_2+b_3)=1$. Таким образом, $f(W, W)\neq 0$, и, следовательно, W — не строго изотропное подпространство. Из равенств $f(b_i, b_i)=1$ вытекает, что σ не является нуль-системой; этим наше предложение полностью доказано.

Следствие 2. *Если характеристика тела F отлична от 2 и полярное отображение σ линейного многообразия (F, A) не является нуль-системой, то подпространство U F-пространства A тогда и только тогда будет N-подпространством, когда оно строго изотропно.*

Доказательство. Выше было отмечено, что каждое строго изотропное подпространство является N-подпространством. Обратное утверждение о строгой изотропности всех N-подпространств можно вывести из предложения 1, поскольку, по условию, σ не является нуль-системой и характеристика тела F отлична от 2.

Легко видеть, что сумма двух N-подпространств F-пространства A не является, вообще говоря, N-подпространством. Поэтому представляет некоторый интерес следующая лемма, которой мы в дальнейшем будем часто пользоваться.

Лемма 3. *Если полярное отображение σ представимо полубилинейной формой f и U, V являются N-подпространствами*

F-пространства A, причем $V \leqslant U + U^{\sigma}$, то $U+V$ будет N-подпространством.

Доказательство. Если элемент x принадлежит $U+V$, то $x=u=v$, где $u \in U$ и $v \in V$. Так как $V \leqslant U+U^{\sigma}$, то $v=u'+w$, где $u' \in U$ и $w \in U^{\sigma}$. Так как подпространства U и V обладают свойством (N), то

$$0=f(v, v)=f(u, u)=f(u', u')=f(u+u', u+u').$$

В то же время, принимая во внимание, что σ есть полярное отображение и элемент w содержится в U^{σ}, и используя лемму 1 (§ 3), мы получаем, что

$$0=f(w, u)=f(u, w)=f(w, u')=f(u', w).$$

Поэтому

$$0=f(v, v)=f(u'+w, u'+w)=$$
$$=f(u', u')+f(u', w)+f(w, u')+f(w, w)=f(w, w),$$
$$f(x, x)=f(u+v, u+v)=f(u+u'+w, u+u'+w)=0,$$

т. е. точка Fx принадлежит своей поляре $(Fx)^{\sigma}$ и, следовательно, подпространство $U+V$ обладает свойством (N).

Если σ — полярное отображение линейного многообразия (F, A), то через $N(\sigma)$ мы будем обозначать *сумму всех неизотропных N-подпространств F-пространства A; дефектом полярного отображения* σ назовем число $n(\sigma)=r[N(\sigma)/(N(\sigma) \cap N(\sigma)^{\sigma})]$.

Предложение 2. *Если σ — полярное отображение линейного многообразия (F, A), то $N(\sigma)$ является N-подпространством и каждое максимальное неизотропное N-подпространство M F-пространства A удовлетворяет условиям*

$$N(\sigma)=M \dotplus [N(\sigma) \cap N(\sigma)^{\sigma}], \quad r(M)=n(\sigma).$$

Доказательство. Если σ является нуль-системой, то A — единственное максимальное неизотропное N-подпространство, так что в этом случае справедливость нашего предложения очевидна. Тривиален также случай, когда 0 является единственным неизотропным N-подпространством F-пространства A. Поэтому можно предположить, что σ не является нуль-системой и что в A существует неизотропное N-подпространство $W \neq 0$. Так как W не может быть точкой, то $1<r(W)<r(A)$. Поэтому $r(A) \geqslant 3$, и, в силу предложения 1 (§ 1), σ представимо полубилинейной формой. Теперь, пользуясь конечностью ранга $r(A)$ (теорема существования, § 1) и леммой 3, а также принимая во внимание, что $A=X \dotplus X^{\sigma}$ для каждого неизотропного подпространства X F-пространства A, мы выведем, что $N(\sigma)$, как сумма конечного числа неизотропных N-подпространств, будет N-подпространством. Так

как каждое максимальное неизотропное N-подпространство M F-пространства A содержится в $N(\sigma)$, то, в силу предложения 2 (§ 2), $N(\sigma) = M \dotplus [N(\sigma) \cap N(\sigma)^\sigma]$. Отсюда следует, что $r(M) = n(\sigma)$.

Замечание 1. Если U — неизотропное N-подпространство и V — произвольное N-подпространство, то из равенства $A = U + U^\sigma$ и леммы 3 следует, что $U + V$ будет N-подпространством. Поэтому, если V есть максимальное N-подпространство F-пространства A, то U будет содержаться в V; отсюда вытекает, что $N(\sigma)$ является частью каждого максимального N-подпространства линейного многообразия (F, A).

Следствие 3. *Дефект $n(\sigma)$ всегда является четным числом, и если характеристика тела F отлична от 2, то либо $n(\sigma) = 0$, либо $n(\sigma) = r(A)$.*

Это утверждение вытекает из предложения 1 § 2 и предложений 1 и 2 этого параграфа.

Для получения особенно простого представления полярного отображения нужно специальным образом выбрать базис F-пространства A. С этой целью совокупность точек $P_1, \ldots, P_k$ назовем *0-множеством точек* (относительно полярного отображения σ), если

$$P_i \leqslant P_j^\sigma \text{ тогда и только тогда, когда } i \neq j. \tag{0}$$

Например, если полярное отображение σ представимо полубилинейной формой f, то точки $Fp_1, \ldots, Fp_k$ тогда и только тогда образуют 0-множество, когда

$$f(p_i, p_j) \begin{cases} \neq 0 & \text{для } i = j, \\ = 0 & \text{для } i \neq j. \end{cases}$$

[Читатель легко заметит связь между этим понятием и понятием ортогональности (см. также ниже § 5).]

Лемма 4. *Пусть σ — полярное отображение линейного многообразия (F, A). Тогда:*

(а) *Если точки $P_1, \ldots, P_k$ образуют 0-множество, то они независимы, а подпространство $\sum_{i=1}^{k} P_i$ неизотропно.*

(б) *0-множество точек $P_1, \ldots, P_k$ максимально тогда и только тогда, когда $[\sum_{i=1}^{k} P_i]^\sigma$ является N-подпространством.*

(в) *Если M есть максимальное неизотропное N-подпространство F-пространства A, то существует такое 0-множество точек $Q_1, \ldots, Q_h$, что $M = [\sum_{i=1}^{h} Q_i]^\sigma$.*

Доказательство. Если точки $P_1, \ldots, P_k$ образуют 0-множество, то $P_i \cap P_i^\sigma = 0$ и $P_i \leqslant P_j^\sigma$ для $i \neq j$. Следовательно,

$$P_i \cap \sum_{i \neq j} P_j = P_i \cap P_i^\sigma \cap \sum_{i \neq j} P_j = 0;$$

этим доказана независимость точек произвольного 0-множества. Далее, используя закон Дедекинда, мы получаем, что

$$[\sum_{j=1}^{i} P_j] \cap P_i^\sigma = [\sum_{j=1}^{i-1} P_j] + (P_i \cap P_i^\sigma) = \sum_{j=1}^{i-1} P_j.$$

Отсюда, пользуясь методом индукции, легко вывести, что

$$[\sum_{j=1}^{k} P_j] \cap [\sum_{j=1}^{k} P_j]^\sigma = [\sum_{j=1}^{k} P_j] \cap P_k^\sigma \cap \ldots \cap P_1^\sigma = \ldots =$$

$$= [\sum_{j=1}^{i} P_j] \cap P_i^\sigma \cap \ldots \cap P_1^\sigma = \ldots = 0.$$

Таким образом, 0-множество порождает неизотропное подпространство; этим утверждение (а) доказано.

Пусть теперь точки $P_1, \ldots, P_k$ образуют 0-множество, и пусть Q — произвольная точка, отличная от всех точек P_i. В таком случае точки $Q, P_1, \ldots, P_k$ тогда и только тогда образуют 0-множество, когда $Q \leqslant [\sum_{i=1}^{k} P_i]^\sigma$ и Q не содержится в Q^σ. Отсюда следует, что 0-множество точек $P_1, \ldots, P_k$ не максимально тогда и только тогда, когда подпространство $[\sum_{i=1}^{k} P_i]^\sigma$ не обладает свойством (N); этим завершается доказательство утверждения (б).

Рассмотрим, наконец, некоторое максимальное неизотропное N-подпространство M F-пространства A. Тогда $A = M \dotplus M^\sigma$. Утверждение (в) безусловно справедливо, если $M^\sigma = 0$; поэтому мы предположим, что $M^\sigma \neq 0$. Подпространство M^σ является одновременно с M неизотропным; поэтому, в силу леммы 1, σ индуцирует в M^σ полярное отображение σ', определяемое равенством

$$U^{\sigma'} = M^\sigma \cap U^\sigma \; [= (M + U)^\sigma]$$

для каждого подпространства U F-пространства M^σ.

Так как пустое множество является 0-множеством, каждое 0-множество, в силу утверждения (а), является независимым множеством точек и из существования полярного отображения следует конечность ранга линейного многообразия (F, M^σ) (теорема существования, § 1), то в M^σ существует максимальное 0-множество точек $Q_1, \ldots, Q_k$ относительно индуцированного полярного

отображения σ'. Очевидно, что эти точки образуют 0-множество и относительно полярного отображения σ. Из утверждений (а) и (б) вытекает, что $V=[\sum_{i=1}^{k} Q_i]^{\sigma'}$ является неизотропным N-подпространством относительно σ', а поэтому и относительно σ. Так как $V\leqslant M^{\sigma}$, то $M\cap V=0$. Покажем теперь, что подпространство $M+V$ обладает свойством (N). Это утверждение очевидно, если M или V совпадает с 0. Если же оба эти подпространства отличны от 0, то их ранги не меньше 2, ибо точки, обладающие свойством (N), изотропны. Следовательно, подпространство $M\dotplus V$, а тем более все A, имеет ранг, не меньший 4; поэтому, в силу предложения 1 (§ 1), σ представимо полубилинейной формой. Теперь, поскольку $M+M^{\sigma}=A$, из леммы 3 вытекает, что $M+V$ обладает свойством (N) и в общем случае. Если положить $W=\sum_{i=1}^{k} Q_i$, то $W^{\sigma'}=V$; поэтому W является одновременно с V неизотропным подпространством относительно σ' и, следовательно, относительно σ. Кроме того, так как $W\leqslant M^{\sigma}$, то $M\leqslant W^{\sigma}$. Отсюда, используя закон Дедекинда, мы получаем, что

$$\begin{aligned}(V+M)\cap(V+M)^{\sigma}&=(M+W^{\sigma'})\cap(M+W^{\sigma'})^{\sigma}=\\&=[M+(W^{\sigma}\cap M^{\sigma})]\cap[M+(W^{\sigma}\cap M^{\sigma})]^{\sigma}=\\&=[M+(W^{\sigma}\cap M^{\sigma})]\cap[M^{\sigma}\cap(W+M)]=\\&=[(M\cap M^{\sigma})+(W^{\sigma}\cap M^{\sigma})]\cap(W+M)=\\&=W^{\sigma}\cap M^{\sigma}\cap(W+M)=W^{\sigma}\cap[W+(M^{\sigma}\cap M)]=\\&=W^{\sigma}\cap W=0,\end{aligned}$$

Таким образом, нами показано, что $M\dotplus V$ является неизотропным N-подпространством. Но M — максимальное подпространство, обладающее этими свойствами; поэтому $V=0$. Следовательно,

$$\sum_{i=1}^{k} Q_i=W=V^{\sigma'}=0^{\sigma'}=M^{\sigma},\ \text{откуда}\ M=[\sum_{i=1}^{k} Q_i]^{\sigma},$$

что и требовалось доказать.

Предложение 3. *Если полярное отображение σ не является нуль-системой и характеристика тела F отлична от 2, то точки каждого максимального 0-множества образуют базис F-пространства A.*

Доказательство. В силу наших предположений и следствия 2, 0 является единственным неизотропным N-подпространством F-пространства A. Поэтому наше предложение непосредственно следует из утверждений (а) и (б) леммы 4.

Замечание 2. В процессе доказательства леммы 4 было показано, что существование максимального 0-множества следует из леммы 4 (а) и конечности ранга линейного многообразия.

Замечание 3. Если условия предложения 3 не выполняются, то либо σ является нуль-системой, и в этом случае пустое множество будет единственным 0-множеством, либо σ не является нуль-системой, но характеристика тела F равна 2. Особенно интересно, что в последнем случае могут существовать два максимальных 0-множества, состоящих из различного числа точек («неинвариантность 0-ранга»); это видно из следующих общих рассмотрений. Как и при доказательстве предложения 1, мы рассмотрим линейное многообразие (F, A) конечного ранга n, не меньшего 3, над полем F характеристики 2, базис $b_1, \ldots, b_n$ этого F-пространства и симметрическую билинейную форму $f(x, y)$, удовлетворяющую условиям

$$f(b_i, b_j) = \begin{cases} 1 & \text{для } i = j, \\ 0 & \text{для } i \neq j. \end{cases}$$

Точки $Fb_1, \ldots, Fb_n$ образуют 0-множество относительно полярного отображения σ, определяемого формой f. Далее, рассмотрим гиперплоскость W, состоящую из всех таких элементов $\sum_{i=1}^{n} x_i b_i$, что $\sum_{i=1}^{n} x_i = 0$. Эта гиперплоскость обладает свойством (N), но не строго изотропна. Поэтому $W = M \dotplus (W \cap W^\sigma)$, где M есть максимальное неизотропное N-подпространство, причем оно отлично от 0. В силу леммы 4 (в), существует такое 0-множество точек $Q_1, \ldots, Q_k$, что $M^\sigma = \sum_{i=1}^{k} Q_i$. Поскольку $r(M) + r(M^\sigma) = n$, мы имеем $k < n$. В то же время из леммы 4 (б) следует, что точки Q_i образуют максимальное 0-множество.

Предложение 4. *Любые два максимальных N-подпространства линейного многообразия (F, A) имеют одинаковые ранги.*

Доказательство. Предложение очевидно, если полярное отображение σ является нуль-системой, так как в этом случае само A будет единственным максимальным N-подпространством. Поэтому предположим, что σ не является нуль-системой. Если A представляет собой прямую, то либо единственным максимальным N-подпространством F-пространства A будет нулевое подпространство [1]), либо максимальными N-подпространствами прямой A будут точки; таким образом, наше предложение для прямых справедливо.

[1]) В этом случае множество точек прямой, остающихся неподвижными при данном полярном отображении, пусто. — *Прим. перев.*

Пусть теперь $r(A) \geqslant 3$. Тогда, в силу предложения 1 (§ 1), σ представимо полубилинейной формой, так что можно пользоваться леммой 3. Пусть W есть максимальное N-подпространство F-пространства A и T — произвольное N-подпространство того же пространства A. Тогда $T' = T \cap (W + W^\sigma)$ будет N-подпространством, содержащимся в $W + W^\sigma$; отсюда и из леммы 3 следует, что $W + T'$ также будет N-подпространством. Но W — максимальное N-подпространство F-пространства A; следовательно, $T' \leqslant W$. Таким образом, нами доказано:

(4.0) Если W есть максимальное N-подпространство F-пространства A и если T — произвольное N-подпространство того же пространства, то $T \cap (W + W^\sigma) \leqslant W$, т. е. $T \cap W = T \cap (W + W^\sigma)$.

[Читатель может проверить, что это утверждение справедливо также и в случаях, когда σ является нуль-системой или когда $r(A) = 2$.]

Предположим теперь, что U и V — максимальные N-подпространства F-пространства A. Тогда, в силу (4.0),

$$U \cap (V + V^\sigma) = U \cap V = V \cap (U + U^\sigma). \qquad \text{(а)}$$

Рассмотрим, кроме того, некоторое максимальное неизотропное N-подпространство M F-пространства A. В силу предложения 2,

$$r(M) = n(\sigma), \qquad \text{(б)}$$

а из леммы 3 или замечания 1 вытекает, что M содержится в U и в V; поэтому, ввиду предложения 2 (§ 2),

$$U = M \dot{+} (U \cap U^\sigma), \quad V = M \dot{+} (V \cap V^\sigma). \qquad \text{(в)}$$

Подставляя теперь (в) в (а) и используя закон Дедекинда, мы получаем, что

$$\left.\begin{aligned} &M + [U \cap U^\sigma \cap (V + V^\sigma)] = (V + V^\sigma) \cap [M + (U \cap U^\sigma)] = \\ &= (V + V^\sigma) \cap U = (U + U^\sigma) \cap V = M + [V \cap V^\sigma \cap (U + U^\sigma)]. \end{aligned}\right\} \qquad \text{(г)}$$

Так как подпространство M неизотропно, то $A = M \dot{+} M^\sigma$ (следствие 2, § 1), а из включений $M \leqslant U$, V вытекает, что $U^\sigma, V^\sigma \leqslant M^\sigma$. Поэтому, беря пересечение обеих частей равенства (г) с подпространством M^σ, получаем, что

$$U \cap U^\sigma \cap (V + V^\sigma) = V \cap V^\sigma \cap (U + U^\sigma); \qquad \text{(д')}$$

применив к этому равенству полярное отображение σ, мы найдем, что

$$U + U^\sigma + (V \cap V^\sigma) = V + V^\sigma + (U \cap U^\sigma). \qquad \text{(д'')}$$

Обозначим через j ранг пересечения (д'), а через s — ранг суммы (д''). Тогда, по формуле для ранга (б) (гл. II, § 2), мы имеем

$$r(U\cap U^\sigma)+r(V+V^\sigma)=j+s=r(V\cap V^\sigma)+r(U+U^\sigma). \qquad \text{(е)}$$

Далее, в силу следствия 1 (§ 1),

$$r(A)=r(U\cap U^\sigma)+r(U+U^\sigma)=r(V\cap V^\sigma)+r(V+V^\sigma), \qquad \text{(ж)}$$

поскольку $(X\cap X^\sigma)^\sigma=X+X^\sigma$. Но из равенств (ж) и (е) вытекает, что

$$r(U\cap U^\sigma)-r(V\cap V^\sigma)=r(V\cap V^\sigma)-r(U\cap U^\sigma),$$

откуда $r(U\cap U^\sigma)=r(V\cap V^\sigma)$. Теперь из равенств (б), (в) и формулы для ранга (б) мы получаем, что

$$r(U)=n(\sigma)+r(U\cap U^\sigma)=n(\sigma)+r(V\cap V^\sigma)=r(V),$$

чем и завершается доказательство предложения 4.

Равные между собой ранги всех максимальных N-подпространств относительно полярного отображения σ мы будем обозначать через $j(\sigma)$. Так как каждое максимальное неизотропное N-подпространство F-пространства A содержится в каждом максимальном N-подпространстве, то $n(\sigma)\leqslant j(\sigma)$; разность $i(\sigma)=j(\sigma)-n(\sigma)$ называется *индексом полярного отображения* σ. Принимая теперь во внимание равенства (в), выведенные в процессе доказательства предыдущего предложения, получаем

Следствие 4. *Если V есть максимальное N-подпространство и M — максимальное неизотропное N-подпространство [относительно данного полярного отображения σ линейного многообразия (F, A)], то*

$$V=M\dotplus(V\cap V^\sigma),\quad r(M)=n(\sigma),\quad r(V)=n(\sigma)+i(\sigma),\quad r(V\cap V^\sigma)=i(\sigma).$$

Таким образом, $i(\sigma)$ есть ранг максимального строго изотропного подпространства.

σ-РАЗЛОЖЕНИЕ ПРОСТРАНСТВА

Мы теперь все подготовили для того, чтобы получить разложение F-пространства A, тесно связанное с данным полярным отображением. Благодаря этому разложению становятся очевидными некоторые характерные свойства этого полярного отображения; в то же время оно позволяет привести к особенно простому виду полубилинейную форму, представляющую наше полярное отображение.

Пусть σ — полярное отображение линейного многообразия (F, A), не являющееся нуль-системой, и пусть $r(A)\geqslant 3$, так что, в силу предложения 1 (§ 1), σ представимо полубилинейной формой.

Заметим, кроме того, что, по теореме существования (§ 1), ранг $r(A)$ конечен. Последнее обстоятельство гарантирует нам существование в F-пространстве A максимальных подпространств, обладающих каким-либо данным свойством.

Обозначим через W некоторое максимальное N-подпространство F-пространства A, а через M — некоторое максимальное неизотропное N-подпространство F-пространства A. В силу замечания 1, $M \leqslant W$, а из следствия 4 вытекает, что

$$(4.1)\quad W = (W \cap W^\sigma) \dotplus M,\quad r(M) = n(\sigma),\quad r(W \cap W^\sigma) = i(\sigma).$$

В A существует такое подпространство J, что $W^\sigma = (W \cap W^\sigma) \dotplus J$. Докажем, что

(4.2) J не содержит ни одного N-подпространства, отличного от 0.

Действительно, пусть V есть N-подпространство, содержащееся в J. Тогда $V \leqslant J \leqslant W^\sigma \leqslant W + W^\sigma$, откуда по лемме 3, следует, что $V + W$ является N-подпространством. Но W — максимальное N-подпространство F-пространства A; поэтому $V \leqslant W \cap J = W \cap W^\sigma \cap J = 0$, что и требовалось доказать.

(4.3) Подпространство J неизотропно.

Это утверждение следует из утверждения (4.2), так как, по лемме 2, подпространство $J \cap J^\sigma$ строго изотропно.

(4.4) $J \cap M = 0$ и $J \dotplus M$ является неизотропным подпространством.

Действительно, $J \cap M$ содержится в N-подпространстве M и поэтому является N-подпространством. Но $J \cap M$ содержится также в J; отсюда и из утверждения (4.2) вытекает, что $J \cap M = 0$. Далее, так как $J \leqslant W^\sigma$, $M \leqslant W$, то, используя, кроме того, закон Дедекинда, мы получаем, что $J \leqslant M^\sigma$ и

$$(J + M) \cap (J + M)^\sigma = (J + M) \cap J^\sigma \cap M^\sigma =$$
$$= [J + (M \cap M^\sigma)] \cap J^\sigma = J \cap J^\sigma = 0,$$

так как M и J — неизотропные подпространства. Следовательно, подпространство $M + J$ также неизотропно.

(4.5) Каждое максимальное 0-множество точек, содержащихся в J, образует базис подпространства J.

Так как J — неизотропное подпространство, то, по лемме 1, σ индуцирует в J полярное отображение σ'. Ввиду этого замечания, утверждение (4.5) непосредственно следует из утверждения (4.2) и леммы 4.

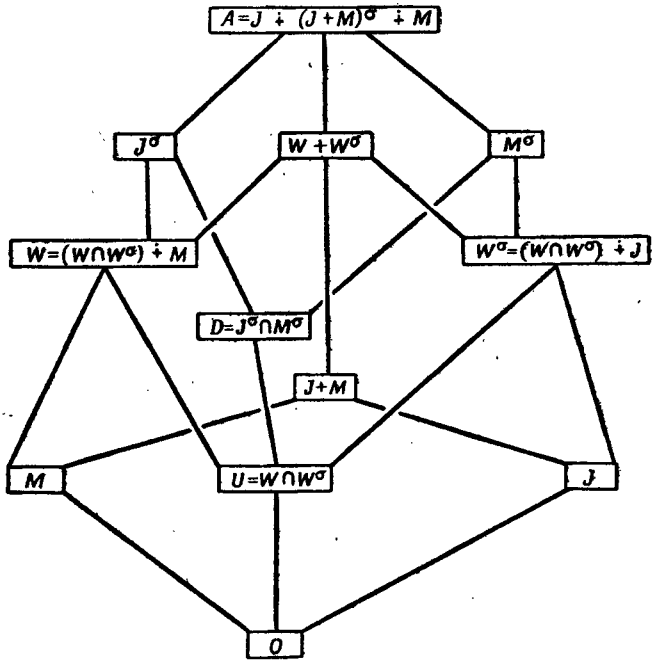
$$(4.6)\quad A = J \dotplus M \dotplus (J + M)^\sigma,\quad W \cap W^\sigma = (W + W^\sigma) \cap J^\sigma \cap M^\sigma.$$

Действительно, из утверждения (4.1) и выбора подпространства J становится очевидным, что $W + W^\sigma = M \dotplus (W \cap W^\sigma) + J$.

Поэтому $W \cap W^\sigma = (W + W^\sigma)^\sigma = M^\sigma \cap (W \dotplus W^\sigma) \cap J^\sigma$. Далее, заметим, что $J \leqslant W^\sigma$ и, следовательно, $M \leqslant W \leqslant J^\sigma$. Отсюда, используя закон Дедекинда, получаем, что

$$M \dotplus (J + M)^\sigma = M \dotplus (J^\sigma \cap M^\sigma) = J^\sigma \cap (M \dotplus M^\sigma) = J^\sigma \cap A = J^\sigma,$$

так как, ввиду неизотропности подпространства M, $A = M \dotplus M^\sigma$. Поскольку $M \cap M^\sigma = 0$, мы имеем $M \cap (J + M)^\sigma = 0$; тем самым



Фиг. 9.

показано, что $J^\sigma = M \dotplus (J + M)^\sigma$. Наконец, так как J — неизотропное подпространство, то

$$A = J \dotplus J^\sigma = J \dotplus M \dotplus (J + M)^\sigma,$$

и этим утверждение (4.6) полностью доказано[1]).

(4.7) $W \cap W^\sigma \leqslant J^\sigma \cap M^\sigma$.

Это включение следует, например, из включения $J + M \leqslant W + W^\sigma$ или из утверждения (4.6).

---

[1]) Первое равенство (4.6) можно непосредственно получить из утверждения (4.4) и следствия 2 (§ 1). — *Прим. перев.*

Из леммы 2 и следствия 4 вытекает такое предложение:

(4.8) Подпространство $W \cap W^\sigma$ строго изотропно; $r(W \cap W^\sigma) = i(\sigma)$.

Строение подпространств J, M, $W \cap W^\sigma$ относительно данного полярного отображения σ по существу описывается соответственно утверждениями (4.2) и (4.5), предложением 1 (§ 2) и утверждением (4.8). Однако мы еще не имеем достаточного представления о строении подпространства $J^\circ \cap M^\circ$ относительно содержащегося в нем подпространства $W \cap W^\sigma$.

(4.9) $W \cap W^\sigma$ является максимальным N-подпространством, содержащимся в $J^\circ \cap M^\circ$.

В самом деле, пусть V — такое N-подпространство, что $W \cap W^\sigma \leqslant V \leqslant J^\circ \cap M^\circ$. Тогда $J + M \leqslant V^\sigma$ и, следовательно,

$$W \leqslant W + W^\sigma = J + M + (W \cap W^\sigma) \leqslant V^\sigma + V.$$

Отсюда и из леммы 3 вытекает, что $V + W$ будет N-подпространством. Но так как W — максимальное N-подпространство, то $V \leqslant W$. Поэтому

$$V \leqslant W \cap M^\sigma \cap J^\sigma \leqslant (W + W^\sigma) \cap M^\sigma \cap J^\sigma = W \cap W^\sigma;$$

последнее равенство имеет место в силу утверждения (4.6). Следовательно, $V = W \cap W^\sigma$.

Так как, в силу утверждения (4.4), подпространство $J + M$ неизотропно, то и подпространство $J^\sigma \cap M^\sigma = (J + M)^\sigma$ также неизотропно. Поэтому, как следует из леммы 1, σ индуцирует в $D = J^\sigma \cap M^\sigma$ полярное отображение δ. Полагая $U = W \cap W^\sigma$, докажем, что

(4.10) $U = U^\delta$, $r(D) = 2r(U)$.

Действительно, в силу утверждения (4.6),

$$U^\delta = (W \cap W^\sigma)^\delta = (W \cap W^\sigma)^\sigma \cap D = (W^\sigma + W) \cap J^\sigma \cap M^\sigma = W \cap W^\sigma = U.$$

Отсюда и из следствия 1 (§ 1) вытекает, что $r(D) = r(U) + r(U^\delta) = 2r(U)$.

(4.11) Существует такое неизотропное подпространство V, что $D = U \dotplus V$.

Прежде всего заметим, что подпространство, содержащееся в D, тогда и только тогда неизотропно относительно σ, когда оно неизотропно относительно δ. В F-пространстве D существует неизотропное подпространство X, удовлетворяющее условию $U \cap X = 0$. Ввиду этого и конечности ранга $r(D)$, в D существует максимальное неизотропное подпространство V, удовлетворяющее условию $U \cap V = 0$. Так как подпространство V неизотропно, то, в силу следствия 2 (§ 1), $D = V \dotplus V^\delta$; с другой стороны, из

утверждения (4.10) и соотношения $U \cap V = 0$ вытекает, что

$$D = 0^{\delta} = U + V^{\delta}.$$

Допустим, что V^{δ} не содержится в $U+V$. Тогда в V^{δ} существуют точки, не принадлежащие $U+V$. Предположим, что одна из точек — обозначим ее через P — не обладает свойством (N). Поскольку $V < V+P$, подпространство $V+P$ либо изотропно, либо удовлетворяет условию $U \cap (V+P) \neq 0$. Но используя закон Дедекинда, мы получаем, что

$$(V+P) \cap (V+P)^{\delta} = (V+P) \cap V^{\delta} \cap P^{\delta} = [P + (V \cap V^{\delta})] \cap P^{\delta} = P \cap P^{\delta} = 0,$$

ибо V и P — неизотропные подпространства; следовательно, наша первая альтернатива не имеет места. Также несправедлива и вторая альтернатива, поскольку

$$U \cap (V+P) = U \cap (U+V) \cap (V+P) = \\ = U \cap [V + ([U+V] \cap P)] = U \cap V = 0.$$

Тем самым показано, что каждая точка подпространства V^{δ}, не содержащаяся в $U+V$, будет N-точкой.

Предположим опять, что P есть точка, содержащаяся в V^{δ} и не содержащаяся в $U+V$. Заметим, что так как полярное отображение σ не является нуль-системой и ранг линейного многообразия (F, A) больше 2, то σ представимо симметрической α-формой f (предложение 1, § 1, и теорема 1, § 3); очевидно, что полярное отображение δ, индуцированное в D полярным отображением σ, представимо той же α-формой f. Пусть теперь t — отличный от 0 элемент тела F, w — элемент из $(U+V) \cap V^{\delta}$ и p — такой (фиксированный) элемент, что $P = Fp$. Тогда точка $F(w+tp)$ содержится в V^{δ}, но не содержится в $(U+V) \cap V^{\delta}$ и, следовательно, является N-точкой. Таким образом, $f(p, p) = 0$ и

$$f(w+tp, w+tp) = f(w, w) + f(w, tp) + f(tp, w) + tf(p, p)\, t^{\alpha} = \\ = f(w, w) + tf(p, w) + [tf(p, w)]^{\alpha} = 0.$$

Поэтому, если $f(p, w) = 0$, то и $f(w, w) = 0$; если же $f(p, w) \neq 0$, то, полагая $t = -f(p, w)^{-1}$, мы получаем, что $f(w, w) = 2$. Тем самым для случая, когда характеристика основного тела равна 2, мы опять получаем, что $f(w, w) = 0$. В случае же, когда характеристика тела F отлична от 2, положив $t = +f(p, w)^{-1}$, найдем, что $f(w, w) = -2$, и поэтому придем к противоречию. Таким образом, показано, что в любом случае $f(w, w) = 0$. Но это означает, что каждая точка подпространства $(U+V) \cap V^{\delta}$ является N-точкой. Так как мы уже раньше установили, что каждая точка

подпространства V^δ, не принадлежащая $U+V$, является N-точкой, то тем самым показано, что любая точка подпространства V^δ есть N-точка. Отсюда и из леммы 3, принимая во внимание, что

$$U \leqslant D = V \dotplus V^\delta,$$

мы получаем, что $U+V^\delta = D$ является N-подпространством. Но в силу утверждения (4.9), U есть максимальное N-подпространство, содержащееся в D. Следовательно, $U=D$, и потому $V^\delta \leqslant U$. Таким образом, предполагая, что V^δ не содержится в $U+V$, мы пришли к противоречию; следовательно, V^δ содержится в $U+V$, и поэтому $D = V \dotplus V^\delta = U \dotplus V$. Этим утверждение (4.11) полностью доказано.

Замечание 4. Стоит отметить, что в процессе доказательства утверждения (4.11) была использована лишь максимальность подпространства V среди неизотропных подпространств, удовлетворяющих условию $U \cap V = 0$.

(4.12) Если V — такое неизотропное подпространство, что $D = U \dotplus V$, $V_1, \ldots, V_k$ — максимальное 0-множество точек, содержащееся в V, $U_i = U \cap (V_i + V^\delta)$ и $W_i = V^\delta \cap (U + V_i)$, то:

(а) $D = U \dotplus V = V \dotplus V^\delta = V^\delta \dotplus U$.

(б) $U_i + V_i = V_i + W_i = W_i + U_i$.

(в) U_i являются точками, образующими базис подпространства U, V_i являются точками, образующими базис подпространства V, и W_i являются точками, образующими базис подпространства V^δ.

(г) Объединение точек V_i и W_i является 0-множеством точек, содержащимся в D.

Действительно, так как $D = U \dotplus V$, то, в силу утверждения (4.10), $D = U^\delta \dotplus V^\delta = U \dotplus V^\delta$, а из неизотропности подпространства V и следствия 2 (§ 1) вытекает, что $D = V \dotplus V^\delta$. Таким образом, утверждение (а) доказано.

Чтобы доказать утверждение (в), положим $T = \sum_{i=1}^{k} V_i$. Тогда $T \leqslant V$ и, по лемме 4 (а), точки V_i образуют базис подпространства T. Далее, из утверждений (а) и (б) леммы 4 следует, что $T^\delta \cap V$ является неизотропным N-подпространством, содержащимся в V. Отсюда и из леммы 3 вытекает, что $U + (V \cap T^\delta)$ будет N-подпространством F-пространства D. Но, в силу утверждения (4.9), U — максимальное N-подпространство F-пространства D; следовательно, $V \cap T^\delta \leqslant U$, и теперь из соотношения $U \cap V = 0$ вытекает, что $V \cap T^\delta = 0$. Так как, в силу леммы 4 (а), T есть неизотропное подпространство, то $D = T \dotplus T^\delta$ (следствие 2, § 1); отсюда и из

включения $T \leqslant V$ вытекает, что $V = T \dotplus (V \cap T^\delta) = T = \sum_{i=1}^{k} V_i$. Теперь, используя теорему об изоморфизме, мы последовательно выведем, что так как V является прямой суммой точек V_i, то фактор-пространство $(U+V)/U = D/U$ разлагается в прямую сумму точек $(U+V_i)/U$; отсюда и из равенства $D = U \dotplus V^\delta$ следует, что подпространство V^δ является прямой суммой точек $(U+V_i) \cap V^\delta = W_i$. Подобным же образом, так как $D/V^\delta = (V+V^\delta)/V^\delta$ разлагается в прямую сумму точек $(V^\delta + V_i)/V^\delta$ и так как $D = U \dotplus V^\delta$, то подпространство U является прямой суммой точек $(V^\delta + V_i) \cap U = U_i$. Этим утверждение (в) доказано; заметим, что, в силу утверждений (а) и (в), $r(U) = r(V) = r(V^\delta) = k$ и $2k = r(D)$.

Используя закон Дедекинда, мы получаем

$$V_i + W_i = V_i + [(U+V_i) \cap V^\delta] = (U+V_i) \cap (V_i + V^\delta) = \\ = V_i + [(V^\delta + V_i) \cap U] = V_i + U_i;$$

отсюда следует утверждение (б), поскольку каждая из точек U_i, V_i, W_i принадлежит одному из попарно дополняющих друг друга подпространств U, V, V^δ и поэтому эти точки попарно различны.

Так как точки V_i образуют 0-множество, то

$$V_i \cap V_j^\delta = \begin{cases} V_i & \text{для } i \neq j, \\ 0 & \text{для } i = j. \end{cases}$$

Из определения точек W_i вытекает, что $W_i \leqslant V^\delta \leqslant V_j^\delta$ и, следовательно, $V_j \leqslant W_i^\delta$. Таким образом, для того чтобы доказать утверждение (г), достаточно проверить, что точки W_i составляют 0-множество. Воспользовавшись законом Дедекинда и утверждением (4.10), получим:

$$W_j \cap W_i^\delta = V^\delta \cap (U+V_j) \cap [V + (U \cap V_i^\delta)] = \\ = V^\delta \cap ([(U+V_j) \cap V] + [U \cap V_i^\delta]) = \\ = V^\delta \cap [V_j + (U \cap V_i^\delta)] = \qquad \text{(так как } U \cap V = 0\text{)} \\ = V^\delta \cap (V^\delta + V_j) \cap [V_j + (U \cap V_i^\delta)] = \\ = V^\delta \cap [V_j + ([V^\delta + V_j] \cap [U \cap V_i^\delta])] = \\ = V^\delta \cap [V_j + [(V^\delta + [V_j \cap V_i^\delta]) \cap U]].$$

Отсюда получаем, что если $j = i$, то

$$W_i \cap W_i^\delta = V^\delta \cap [V_i + (V^\delta \cap U)] = V^\delta \cap V_i = 0;$$

если же $j \neq i$, то

$$W_j \cap W_i^\delta = V^\delta \cap [V_j + ([V^\delta + V_j] \cap U)] = V^\delta \cap (V_j + U) \cap (V^\delta + V_j) = W_j,$$

и этим утверждение (4.12) полностью доказано.

В заключение подытожим полученные результаты и посмотрим, что следует из них для симметрической α-формы f, представляющей полярное отображение σ.

1. *Максимальное неизотропное N-подпространство M F-пространства A.*

Ранг этого подпространства равен *дефекту* $n(\sigma)$, а f является на M кососимметрической билинейной формой. При соответствующем выборе базиса подпространства M форму f можно привести на M к следующему нормальному виду:

$$f(x, y) = \sum_{i=1}^{h} [x_{2i-1} y_{2i} - x_{2i} y_{2i-1}],$$

где $2h = n(\sigma)$ [см. формулу (1*), стр. 138].

2. *Максимальное строго изотропное N-подпространство F-пространства A.*

Это подпространство в предыдущем рассмотрении обозначалось через $U = W \cap W^\sigma$; его ранг равен *индексу* $i(\sigma)$, а форма f на U тождественно равна 0.

3. *Неизотропная оболочка максимального строго изотропного подпространства.*

Это подпространство в предыдущем рассмотрении обозначалось через $D = J^\sigma \cap M^\sigma$; его ранг равен $2i(\sigma)$. Если в качестве базиса подпространства D выбрать 0-множество точек V_i, W_i [о которых говорилось в утверждении (4.12)], то, как легко проверить, форму f на D можно привести к следующему нормальному виду:

$$f(x, y) = \sum_{i=1}^{k} [x_{2i-1} c_i y^\alpha_{2i-1} - x_{2i} c_i y^\alpha_{2i}],$$

где $k = i(\sigma)$ и $c_i = c_i^\alpha \neq 0$.

4. *Компонента, свободная от N-подпространств.*

Это подпространство мы обозначали через J. Из утверждения (4.6) и других замечаний следует, что $r(J) = n - n(\sigma) - 2i(\sigma)$. В качестве базиса подпространства J можно выбрать максимальное 0-множество точек, содержащееся в J. При таком выборе базиса форма f примет на J следующий нормальный вид:

$$f(x, y) = \sum_{i=1}^{l} x_i d_i y_i^\alpha,$$

где $l = n - n(\sigma) - 2i(\sigma)$, $d_i = d_i^\alpha \neq 0$, причем из $f(x, x) = 0$ для x из J следует, что $x = 0$. Поэтому можно сказать, что форма f

является в некотором смысле (положительно или отрицательно) определенной на J.

Коэффициенты c_i и d_j, встречающиеся в приведенных выше формулах, определяются далеко не однозначно, поскольку их всегда можно заменить коэффициентами $t_i c_i t_i^{\alpha}$ и $s_j d_j s_j^{\alpha}$. Описание полуторалинейных форм при помощи инвариантов является одной из интереснейших областей исследования; читатель может познакомиться с этим вопросом, например, по работе Витта [1] и монографиям Дьёдонне [1, 2], Хуа Ло-гэна [3], Вейля [1]. Изучению несколько особой ситуации, имеющей место в том случае, когда характеристика основного тела равна 2, посвящена, например, работа Арфа [1].

Добавление I

Закон инерции Сильвестра

Если α — инволюторный инверсный автоморфизм тела F, то подмножество P элементов из F мы назовем *областью α-положительности* тела F, если оно обладает следующими свойствами:

(а) P содержит 1 и не содержит 0.

(б) Если P содержит x и y, то P содержит $x+y$.

(в) Если P содержит x, то $x^{\alpha}=x$.

(г) Если $x=x^{\alpha}\neq 0$ не содержится в P, то P содержит $-x$.

(д) Если x содержится в P и $y\neq 0$ — произвольный элемент тела F, то P содержит yxy^{α}.

Пример. Если F есть поле комплексных чисел (или тело действительных кватернионов) и если x^{α} — комплексно сопряженное к x число, то единственной областью α-положительности поля F будет множество положительных действительных чисел.

Замечание 1. Если, в частности, α — тождественный автоморфизм[1]), то область 1-положительности очень похожа на то, что мы раньше, в добавлении III к гл. III, называли областью положительности. Однако из свойств (а) — (д) не следует, вообще говоря, что произведение чисел, принадлежащих P, также содержится в P.

Замечание 2. Если P есть область положительности (в смысле добавления III к гл. III), то P будет также областью 1-положительности[2]).

Замечание 3. Если P — такая область положительности тела F, что $P^{\alpha}=P$, и если Q — множество всех элементов q из P, удовлетворяющих условию $q^{\alpha}=q$, то Q будет областью α-положительности.

Из свойств (а), (б) и (д) непосредственно вытекает следующее свойство области α-положительности.

---

[1]) Что возможно лишь в случае, когда F — поле. — *Прим. перев.*

[2]) Если F — поле. — *Прим. перев.*

(е) *Если* $y_1, \ldots, y_k$ *— отличные от* 0 *числа тела* F, *то число* $\sum_{i=1}^{k} y_i y_i^{\alpha}$ *принадлежит* P.

Отсюда следует, что такая сумма отлична от 0; это показывает, что характеристика тела F равна 0 (так что, в частности, $+1 \neq -1$).

Замечание 4. Отметим, что в теле F может существовать несколько областей α-положительности. Если, например, η — такой автоморфизм тела F, что $\alpha\eta = \eta\alpha$, то одновременно с P областью α-положительности будет и множество P^{η}.

Пусть теперь σ — полярное отображение F-пространства A, ранг которого не меньше 3. Возможно, что σ является нуль-системой; этот случай мы из наших рассмотрений исключаем. Тогда, если характеристика тела F отлична от 2, то, в силу предложения 2 и следствия 3 (§ 4), 0 будет единственным неизотропным N-подпространством F-пространства A. Далее, согласно теореме 1 (§ 3), σ можно представить такой α-формой $f(x, y)$, что α будет инволюторным инверсным автоморфизмом тела F и $f(x, y)^{\alpha} = f(y, x)$ для любых x и y из A.

Предположим теперь, что нам дана некоторая определенная область P α-положительности тела F; все наши последующие определения и рассмотрения зависят от выбора α, P и f.

Если $X = Fx$ — некоторая точка F-пространства A, то возможны следующие три случая.

Случай 1: $f(x, x)$ содержится в P. Если t — произвольное отличное от 0 число из F, то $f(tx, tx) = tf(x, x)t^{\alpha}$; следовательно, в силу свойства (д), $f(tx, tx)$ также содержится в P. Таким образом, $f(y, y)$ принадлежит P для каждого такого y, что $X = Fy$; в этом случае мы будем называть точку X *положительной*.

Случай 2: $f(x, x) = 0$. Этот случай возможен тогда и только тогда, когда X содержится в X^{σ}, т. е. когда X является N-*точкой*.

Случай 3: $f(x, x) \neq 0$ и не содержится в P. Из симметричности формы f следует, что $f(x, x)^{\alpha} = f(x, x)$; поэтому, в силу свойства (г), P содержит $-f(x, x)$. Отсюда, так же как и в случае 1, мы получим, что $-f(y, y)$ содержится в P для любого такого y, что $X = Fy$; такую точку X мы будем называть *отрицательной*.

Очевидно, что свойство быть N-точкой зависит только от σ. Если же мы заменим форму f формой $-f$, то это не приведет к каким-либо существенным изменениям, однако положительные точки станут отрицательными и наоборот. Из предложения 3 (§ 1) следует, что при замене формы f другой симметрической формой, представляющей полярное отображение σ, может произойти только такого рода изменение[1]). Таким образом, наше разбиение всех

[1]) Следующий пример показывает, что это утверждение в общем случае верно. Пусть $F = Q\{u\}$ — поле степенных рядов над полем Q, которое в свою

точек F-пространства A на три класса зависит (с точностью до названия класса) только от σ и P.

При выборе другой области α-положительности наше разбиение точек на классы может существенно измениться, за исключением класса N-точек, которые останутся N-точками.

Теорема Сильвестра. *Число положительных точек одно и то же для любых двух максимальных* 0*-множеств относительно полярного отображения* σ.

Доказательство. Пусть $P_1, \ldots, P_m$ и $Q_1, \ldots, Q_n$ — два максимальных 0-множества точек относительно полярного отображения σ. Так как характеристика тела F равна 0, то, в силу предложения 3 (§ 4), $m = n = r(A)$ (здесь мы используем также наше предположение о том, что σ не является нуль-системой). Ни одна из точек P_i, Q_j не является N-точкой. Допустим, что точки $P_1, \ldots, P_h$ положительны, а точки $P_{h+1}, \ldots, P_m$ отрицательны; аналогично, пусть точки $Q_1, \ldots, Q_k$ положительны, а $Q_{k+1}, \ldots, Q_m$ отрицательны.

(а) *Каждая точка, содержащаяся в* $P_1 + \ldots + P_h$, *положительна.*

Для того, чтобы это доказать, рассмотрим произвольную точку, содержащуюся в $\sum_{i=1}^{h} P_i$. Ее можно представить в виде Ft, где $t = \sum_{i=1}^{h} t_i$ и t_i принадлежит P_i. Некоторые из элементов t_i могут равняться 0, но не все, поскольку $t \neq 0$. Если $t_i \neq 0$, то $f(t_i, t_i)$ принадлежит P, так как P_i — положительная точка. Поскольку точки P_i образуют 0-множество, мы имеем $f(t_i, t_j) = 0$ для $i \neq j$.

очередь является полем степенных рядов над упорядоченным полем Z $(Q = Z\{t\})$. Элемент a из F, который можно однозначно представить в виде $a = \sum_{i=0}^{\infty} a_i(t)\, u^{k+i}$, где $a_i(t) = \sum_{j=0}^{\infty} a_{ij} t^{l_i + j}$, a_{ij} — элементы из Z, мы назовем положительным, если либо k и l_0 — четные числа и $a_{00} > 0$, либо хотя бы одно из чисел k и l_0 нечетно и $a_{00} < 0$. Нетрудно проверить, что множество P положительных элементов будет областью 1-положительности поля F. В P существуют такие пары элементов, например $-t$, $-u$, произведения которых в P не содержатся; пусть a, b — любая такая пара. Форма $f(x, y) = ax_1y_1 + \sum_{i=2}^{n} x_i y_i$ является обычной билинейной формой, представляющей некоторое полярное отображение n-мерного F-пространства. Относительно формы f каждая точка будет положительной. В то же время относительно формы fb, представляющей то же самое полярное отображение, имеются как положительные, так и отрицательные точки.

В действительности утверждение автора справедливо тогда и только тогда, когда произведение любой пары элементов из области P α-положительности, по крайней мере один из которых перестановочен с каждым элементом из P, принадлежит P. — *Прим. перев.*

Поэтому

$$f(t, t) = \sum_{i=1}^{h} f(t_i, t_i);$$

отсюда и из свойства (б) областей α-положительности следует, что $f(t, t)$ принадлежит P. Таким образом, Ft является положительной точкой.

Подобным же образом можно показать, что

(б) *каждая точка, содержащаяся в* $P_{h+1} + \ldots + P_m$, *отрицательна.*

То же самое справедливо и для точек Q_j, т. е. каждая точка, содержащаяся в $\sum_{i=1}^{k} Q_i$, положительна и каждая точка, содержащаяся в $\sum_{i=k+1}^{m} Q_i$, отрицательна. Отсюда и из утверждений (а) и (б) следует, что

$$[\sum_{i=1}^{h} P_i] \cap [\sum_{i=k+1}^{m} Q_i] = [\sum_{i=h+1}^{m} P_i] \cap [\sum_{i=1}^{k} Q_i] = 0.$$

Однако, по лемме 4 (§ 4), 0-множество точек независимо. Следовательно,

$$h + (m - k) \leqslant r(A) \quad \text{и} \quad (m - h) + k \leqslant r(A).$$

Но $m = r(A)$, поэтому $h - k \leqslant 0$ и $k - h \leqslant 0$, откуда $k = h$, что и требовалось доказать.

Замечание 5. Если через p обозначить число положительных точек во всех максимальных 0-множествах относительно полярного отображения σ (с определенной симметрической α-формой f и определенной областью P α-положительности), то $n = r(A) - p$ будет числом отрицательных точек во всех максимальных 0-множествах. Если мы заменим форму f формой $-f$, то n станет числом положительных точек, а p — числом отрицательных точек во всех максимальных 0-множествах. Таким образом, лишь (неупорядоченная) пара $[p, n]$ является инвариантом полярного отображения σ (при заданной области P α-положительности)[1]. Число $\min(p, n)$ мы назовем *индексом инерции полярного отображения* σ (относительно области P α-положительности)[2]. Так как $p + n = r(A)$, то ясно, что инвариантная пара $[p, n]$ полностью определяется двумя инвариантами: рангом F-пространства A и индексом инерции.

Применение 1. Пусть F есть поле обычных действительных чисел. В этом случае единственным автоморфизмом (и инверсным

[1]) См. примечание на стр. 163. — *Прим. перев.*

[2]) В оригинале индекс инерции определяется как абсолютная величина $|p - n|$ разности чисел p и n. Однако при таком определении индекса инерции оказывается неверным замечание 6. — *Прим. перев.*

автоморфизмом) поля F будет тождественный автоморфизм; поэтому каждая полубилинейная форма над произвольным линейным многообразием (F, A) в действительности будет билинейной формой. Это поле F допускает лишь одну алгебраическую упорядоченность, поскольку множество P всех отличных от 0 квадратов действительных чисел является его единственной областью положительности.

Если теперь нам дана билинейная форма $f(x, y)$, представляющая полярное отображение σ, и если Fx есть точка F-пространства A, то $f(tx, tx) = t^2 f(x, x)$ для любого действительного числа t. Следовательно, каждую положительную точку можно представить в виде Fu, где u — такой элемент, что $f(u, u) = 1$; аналогично, каждая отрицательная точка представима в виде Fv, где v — такой элемент, что $f(v, v) = -1$. Учитывая это, мы обычным способом найдем, что

$$f(x, y) = \sum_{i=1}^{p} x_i y_i - \sum_{i=p+1}^{r(A)} x_i y_i,$$

где p — число положительных точек в максимальных 0-множествах.

Применение 2. Пусть F — тело действительных кватернионов и R — его подполе действительных чисел. Тогда R является центром тела F и любой инверсный автоморфизм тела F оставляет неподвижным каждый элемент из R. Если инволюторный инверсный автоморфизм α тела F оставляет неподвижными только числа из R, то с помощью точно таких же рассуждений, какими мы пользовались в применении 1, можно показать, что симметрическую α-форму f можно привести к следующему нормальному виду:

$$f(x, y) = \sum_{i=1}^{p} x_i y_i^{\alpha} - \sum_{i=p+1}^{r(A)} x_i y_i^{\alpha},$$

где p — также число положительных точек в максимальных 0-множествах.

Замечание 6. В рассмотренных примерах индекс инерции был равен индексу $i(\sigma)$, введенному в § 4. В общем же случае можно только доказать, что $i(\sigma)$ не превышает индекса инерции, причем очень легко построить примеры, в которых индекс инерции строго больше индекса $i(\sigma)$.

Добавление II

Проективные соотношения между прямыми, индуцированные полярными отображениями

Если σ есть полярное отображение линейного многообразия (F, A) и L — прямая этого линейного многообразия, то ранг факторпространства A/L^{σ} равен 2 [так как собственными подпростран-

ствами прямой L являются только точки, то лишь гиперплоскости являются подпространствами, расположенными строго между A и L^σ; но это эквивалентно тому, что $r(A/L^\sigma)=2$]. Если L' — некоторая прямая, удовлетворяющая условию $L'\cap L^\sigma=0$, то из $r(A/L^\sigma)=2$ следует, что $A=L'\dotplus L^\sigma$. Полученное равенство эквивалентно, очевидно, равенству $A=L'^\sigma\dotplus L$; тем самым мы показали, что эквивалентны следующие свойства прямых L и L':

$$L'\cap L^\sigma=0,\quad A=L'\dotplus L^\sigma,\quad A=L\dotplus L'^\sigma,\quad L\cap L'^\sigma=0.$$

Рассмотрим теперь две прямые L и L', удовлетворяющие этим эквивалентным между собой условиям. Если P — точка прямой L, то пересечение $L'\cap P^\sigma=P'$ также представляет собой точку, поскольку гиперплоскость P^σ содержит подпространство L^σ и поэтому

$$P^\sigma=L^\sigma\dotplus(P^\sigma\cap L')=L^\sigma\dotplus P'.$$

Далее, используя закон Дедекинда, получаем

$$L\cap P'^\sigma=L\cap(L'\cap P^\sigma)^\sigma=L\cap(L'^\sigma+P)=P+(L\cap L'^\sigma)=P.$$

Отсюда видно, что отображение точки P прямой L на точку $P'=L'\cap P^\sigma$ прямой L' и отображение точки Q прямой L' на точку $L\cap Q^\sigma$ прямой L являются взаимно обратными отображениями; следовательно, оба эти отображения будут взаимно однозначными отображениями всех точек одной прямой на все точки другой прямой. Такое отображение точек P прямой L на точки $P^\sigma\cap L'$ прямой L' мы назовем *σ-отображением* прямой L на прямую L'; заметим, что σ-отображение можно определить тогда и только тогда, когда $A=L'\dotplus L^\sigma$. Целью настоящего добавления является изучение таких отображений.

Лемма 1. *Пусть полярное отображение σ линейного многообразия (F, A) представимо симметрической α-формой $f(x, y)$, $L=Fp+Fq$ является прямой F-пространства A и прямые L и L' удовлетворяют условию $A=L'\dotplus L^\sigma$. Тогда в A существуют такие элементы p' и q', что*

$$L'=Fp'+Fq',\quad Fp'=L'\cap(Fp)^\sigma,\quad Fq'=L'\cap(Fq)^\sigma,$$
$$F(p'+x^\alpha q')=L'\cap[F(p+xq)]^\sigma$$

для каждого числа x из F.

Доказательство. Для каждой точки P прямой L положим $P'=L'\cap P^\sigma$. Такое сопоставление точке P точки P' является σ-отображением прямой L на прямую L'; так как $A=L'\dotplus L^\sigma$, то, как мы показали выше, это отображение будет

взаимно однозначным отображением всех точек прямой L на все точки прямой L'. Поэтому $(Fp)'$, $(Fq)'$, $[F(p+q)]'$ являются тремя различными точками прямой L' и, как мы неоднократно выше показывали, в F-пространстве A можно выбрать такие элементы p'', q'', что $(Fp)' = Fp''$, $(Fq)' = Fq''$, $[F(p+q)]' = F(p''+q'')$. Так как полярное отображение σ представимо формой f и так как $Fp'' \leqslant (Fp)^{\perp}$, то $f(p, p'') = f(p'', p) = 0$. Если бы $f(p'', q)$ также равнялось 0, то отсюда следовало бы, что $f(p'', L) = 0$, т. е. точка Fp'' принадлежала бы подпространству $L^{\perp}$. Но, по предположению, $L' \cap L^{\perp} = 0$, а точка Fp'' лежит на прямой L'. Таким образом, $t = f(p'', q) \neq 0$, и, следовательно, можно положить $p' = t^{-1}p''$ и $q' = t^{-1}q''$. Тогда, естественно,

$$(Fp)' = Fp', \quad (Fq)' = Fq', \quad [F(p+q)]' = F(p'+q'), \quad f(p', q) = 1,$$

так что, в частности, $L' = Fp' + Fq'$. Так же, как ранее, заметим, что $f(p, p') = f(p', p) = 0$, $f(q, q') = f(q', q) = 0$; используя эти равенства, мы находим, что

$$0 = f(p+q, p'+q') = \\ = f(p, p') + f(p, q') + f(q, p') + f(q, q') = f(p, q') + 1,$$

откуда $f(p, q') = f(q', p) = -1$, ибо, по предположению, f есть симметрическая α-форма и, следовательно, $f(x, y) = f(y, x)^{\alpha}$. Теперь, используя инволюторность инверсного автоморфизма α, мы получаем, что

$$f(p' + x^{\alpha}q', p + xq) = \\ = f(p', p) + f(p', q)\,x^{\alpha} + x^{\alpha} f(q', p) + x^{\alpha} f(q', q)\,x^{\alpha} = x^{\alpha} - x^{\alpha} = 0.$$

Таким образом, точка $F(p' + x^{\alpha}q')$ лежит как на гиперплоскости $[F(p+xq)]^{\perp}$, так и на прямой L'; теперь наша лемма непосредственно следует из того, что σ-отображение прямой L на прямую L' является взаимно однозначным отображением всех точек прямой L на все точки прямой L'.

Предложение 1. *Если ранг линейного многообразия (F, A) не меньше 3 и если полярное отображение σ не является нуль-системой, то*

(а) *σ-отображения прямых тогда и только тогда индуцируются автопроективными отображениями F-пространства A, когда F будет полем;*

(б) *σ-отображения прямых тогда и только тогда индуцируются коллинеациями F-пространства A, когда σ представимо билинейной формой.*

Доказательство. Из теоремы 1 (§ 3) следует, что полярное отображение σ можно представить симметрической α-формой f, где α — инволюторный инверсный автоморфизм тела F. Если L

есть прямая F-пространства A, то в A существует такое подпространство T, что $A = L \dot{+} T$. Естественно, что $L' = T^\sigma$ будет прямой, причем такой, что $A = L \dot{+} L'^\sigma$; этим доказано существование σ-отображения произвольной прямой на некоторую другую прямую.

Из леммы 1 и леммы 3 (гл. III, § 4) вытекает, что σ-отображение одной прямой на другую тогда и только тогда индуцируется автопроективным отображением F-пространства A, когда α является автоморфизмом тела F, и что σ-отображение одной прямой на другую тогда и только тогда индуцируется коллинеацией, когда α является внутренним автоморфизмом тела F. Но инверсный автоморфизм α тела F тогда и только тогда будет автоморфизмом, когда F — поле; аналогично, α тогда и только тогда будет внутренним автоморфизмом, когда F — поле и $\alpha = 1$. Тем самым наше предложение полностью доказано.

Замечание 1. Если прямые L и L' удовлетворяют условию $A = L \dot{+} L'^\sigma$, то, в силу леммы 1 и леммы 2 (гл. III, § 4), равенство

$$\begin{bmatrix} L' \cap P^\sigma & L' \cap Q^\sigma \\ L' \cap S^\sigma & L' \cap R^\sigma \end{bmatrix} = \begin{bmatrix} P & Q \\ S & R \end{bmatrix}^\alpha$$

будет справедливо для любых четырех попарно различных точек P, Q, R, S прямой L, если только полярное отображение σ представимо симметрической α-формой. Таким образом, наряду с автопроективными отображениями, с помощью полярных отображений также можно определенным образом строить отображения точек прямой, сохраняющие сложные отношения.

Предложение 2. *Пусть L есть прямая и σ—полярное отображение линейного многообразия (F, A). Тогда:*

(а) *Если $L \cap L^\sigma$ — точка, то она является единственной N-точкой прямой L.*

(б) *Если σ представимо полубилинейной формой, характеристика тела F отлична от 2 и прямая L проходит только через одну N-точку, то $L \cap L^\sigma$ является точкой.*

Доказательство. Если $P = L \cap L^\sigma$ есть точка, то $0 < L^\sigma$ и $L < A$, так что $r(A) \geqslant 3$. Следовательно, в силу предложения 1 (§ 1), σ представимо полубилинейной формой. Так как $P \leqslant L \leqslant L + L^\sigma = (L^\sigma \cap L)^\sigma = P^\sigma$, то P является N-точкой прямой L. Пусть Q — вторая N-точка прямой L. Тогда $L = P + Q$ и $Q \leqslant L \leqslant P^\sigma$; отсюда и из леммы 3 (§ 4) вытекает, что L является N-прямой. Но в таком случае, в силу следствия 1 (§ 4), $L \cap L^\sigma$ либо равно 0, либо равно L, что противоречит нашему предположению о том,

что $L \cap L^\sigma$ является точкой. Следовательно, P является единственной N-точкой прямой L. Тем самым утверждение (а) доказано.

Пусть теперь полярное отображение σ представимо некоторой полубилинейной формой, характеристика тела F отлична от 2 и прямая L проходит только через одну N-точку P. Прямая L проходит также через некоторую точку $P' \neq P$. Точка P' принадлежит прямой L, но не принадлежит гиперплоскости P'^σ; отсюда, в частности, следует, что P'^σ не содержит всю прямую L. Поэтому пересечение $P'' = L \cap P'^\sigma$ будет точкой, причем отличной от точки P', ибо в противном случае P' была бы N-точкой. Таким образом, либо $P'' = P$, либо, как обычно, найдутся такие элементы p', p'', что $P' = Fp'$, $P = F(p' + p'')$, $P'' = Fp''$. Поскольку P' не является N-точкой, существует α-форма $f(x, y)$, представляющая полярное отображение σ и удовлетворяющая условию $f(p', p') = 1$; из предложения 1 (§ 3) следует, что $f(x, y)$ будет симметрической α-формой и $\alpha^2 = 1$. Так как p'' содержится в P'^σ, то $f(p'', p') = f(p', p'') = 0$; отсюда, принимая во внимание, что P является N-точкой, мы получаем

$$0 = f(p' + p'', p' + p'') = f(p', p') + f(p'', p'') = 1 + f(p'', p''),$$

т. е. $f(p'', p'') = -1$. Поскольку характеристика тела F отлична от 2, точка $F(p' - p'')$ отлична от точки P; но эта точка является, очевидно, N-точкой, так как $f(p' - p'', p' - p'') = 0$. Таким образом, предположение, что $P \neq P''$, приводит нас к противоречию. Следовательно, $P = P'' = L \cap P'^\sigma$. Отсюда и из того, что P является N-точкой прямой L, мы получаем

$$P \leqslant L \cap P^\sigma \cap P'^\sigma = L \cap (P + P')^\sigma = L \cap L^\sigma.$$

В то же время равенство $L = L \cap L^\sigma$ невозможно, ибо в этом случае каждая точка прямой L была бы N-точкой. Так как L является прямой, то из всех наших рассмотрений следует, что $P = L \cap L^\sigma$. Таким образом, утверждение (б) также доказано.

Замечание 2. Если A — плоскость и характеристика тела F отлична от 2, то точка L^σ является полюсом прямой L; из предложения 2 вытекает, что прямая L тогда и только тогда проходит через свой полюс, когда L содержит одну и только одну N-точку.

Замечание 3. Если $A = L$ — прямая, то $L^\sigma = 0$ и каждая перестановка точек прямой L, оставляющая неподвижной только одну точку, представляет собой пример полярного отображения, для которого утверждение (б) неверно. Отсюда видна необходимость предположения, что полярное отображение σ представимо полубилинейной формой, сделанного в формулировке предложе-

ния 2. Заметим, что это предположение выполняется всякий раз, когда $r(A) \geqslant 3$ (см. предложение 1, § 1).

Замечание 4. Если характеристика тела F равна 2, то утверждение (б), вообще говоря, несправедливо; это видно из следующего часто используемого примера. Пусть F — произвольное поле характеристики 2, а (F, A) — плоскость над F. Если представить, что возможно, элементы плоскости A в виде троек $x = (x_1, x_2, x_3)$ чисел x_i из F, то следующим образом можно над A определить билинейную форму:

$$f(x, y) = \sum_{i=1}^{3} x_i y_i.$$

При таком определении формы f точка $F(x_1, x_2, x_3)$ тогда и только тогда будет N-точкой, когда она лежит на прямой $\sum_{i=1}^{3} x_i = 0$, поскольку $f(x, x) = \sum_{i=1}^{3} x_i^2 = \left[\sum_{i=1}^{3} x_i\right]^2$, так как характеристика поля F равна 2. Эта N-прямая L пересекается с каждой другой прямой плоскости A, и, следовательно, каждая прямая, отличная от L, проходит через одну и только одну N-точку. Но полюсом прямой $x_1 = 0$ является точка $F(1, 0, 0)$, не лежащая на своей поляре; таким образом, эта прямая содержит лишь одну N-точку, но не проходит через свой полюс.

Лемма 2. *Инволюторный инверсный автоморфизм α тела F тогда и только тогда является тождественным автоморфизмом, когда*

(а) *из $r \cdot r^\alpha = 1$ следует $r = \pm 1$,*

(б) *если характеристика тела F равна 2, то $xx^\alpha = x^\alpha x$ для каждого x из F.*

Замечание. Пока остается, видимо, открытым вопрос о том, не является ли условие (б) следствием условия (а).

Доказательство. Необходимость наших условий очевидна. Пусть теперь выполняется условие (а). Тогда прежде всего докажем, что

(а.1) *из $xx^\alpha = x^\alpha x$ следует $x^\alpha = \pm x$.*

Действительно, это утверждение справедливо, очевидно, если $x = 0$; поэтому можно предположить, что $x \neq 0$. В таком случае можно положить $r = x^{-1}x^\alpha$. Так как элементы x и x^α перестановочны, то

$$rr^\alpha = x^{-1}x^\alpha x x^{-\alpha} = 1.$$

Следовательно, в силу условия (а), $r = \pm 1$, что, очевидно, эквивалентно равенству $x^\alpha = \pm x$.

Если характеристика тела F равна 2, то тождественность инверсного автоморфизма α теперь непосредственно следует из (а.1) и (б), а тем самым из (а) и (б).

Таким образом, остается рассмотреть случай, когда характеристика тела F отлична от 2. Если t — произвольный элемент из F, то элемент $s=(t^\alpha-t)-1$ перестановочен, очевидно, с элементом

$$s^\alpha=t-t^\alpha-1=-(t^\alpha-t)-1=-s-2.$$

Отсюда и из утверждения (а.1) следует, что

$$t-t^\alpha-1=s^\alpha=\pm s=\pm(t^\alpha-t-1).$$

В полученном равенстве знак минус перед скобкой невозможен, так как в этом случае мы имели бы $-1=+1$, а это противоречит нашему предположению о том, что характеристика тела F отлична от двух. Следовательно, $t-t^\alpha-1=t^\alpha-t-1$, или $2t^\alpha=2t$; отсюда вытекает, что $t^\alpha=t$, ибо, по предположению, характеристика тела F отлична от 2. Таким образом, мы показали, что $\alpha=1$, чем лемма и доказана.

Предложение 3. *Если ранг линейного многообразия (F, A) не меньше 3 и если относительно полярного отображения σ в A существуют N-точки, то σ тогда и только тогда представимо обычными билинейными формами, когда*

(а) *каждая прямая, содержащая более двух N-точек, является N-прямой и*

(б) *F есть поле.*

Если характеристика тела F отлична от 2, то условие (б) *следует из условия* (а).

Доказательство. Так как $r(A)\geqslant 3$, то, в силу предложения 1 (§ 1), σ представимо полубилинейной формой; заметим, что только здесь мы используем предположение, что $r(A)\geqslant 3$. Из предложения 3 (§ 1) следует, что каждая форма, представляющая полярное отображение σ, будет обычной билинейной формой, если хотя бы одна из таких форм обладает этим свойством.

Пусть σ представимо обычными билинейными формами. Тогда тождественный автоморфизм будет инверсным автоморфизмом тела F и, следовательно, F будет полем. Предположим теперь, что прямая L содержит три попарно различные N-точки P, Q, R. В таком случае существуют такие элементы p, q, что $P=Fp$, $Q=Fq$, $R=F(p+q)$. Поэтому, если f — некоторая билинейная форма, представляющая σ, то

$$0=f(p, p)=f(q, q)=f(p, q)+f(q, p);$$

отсюда, используя коммутативность поля F и билинейность формы f, мы получаем

$$f(xp+yq, xp+yq)=$$
$$=xf(p, p)x+xf(p, q)y+yf(q, p)x+yf(q, q)y=$$
$$=xy[f(p, q)+f(q, p)]=0.$$

Таким образом, L является N-прямой. Этим необходимость условий (а) и (б) полностью доказана. Мы предлагаем читателю рассмотреть связи между условием (а), предложением 1 и тем фактом, что линейное преобразование прямой, оставляющее неподвижными по крайней мере три точки, тождественно.

Пусть теперь выполняется условие (а). В F-пространстве A существует по крайней мере одна N-точка P. Мы будем различать два возможных случая.

Случай 1: каждая точка, не принадлежащая P^σ, является N-точкой. Если Q есть точка гиперплоскости P^σ, отличная от P, то $Q^\sigma \neq P^\sigma$ и поэтому гиперплоскость Q^σ содержит по крайней мере одну точку Q', не принадлежащую P^σ. В таком случае прямая $L = Q + Q'$ не содержится в P^σ и, следовательно, пересекается с P^σ по точке Q. Если $Q = Fq$, $Q' = Fq'$ и $R = F(q + q')$, то, очевидно, точка R одновременно с точкой Q' не содержится в P^σ; таким образом, Q' и R являются N-точками. Поэтому, если f — полубилинейная форма, представляющая полярное отображение σ, то

$$0 = f(q', q) = f(q, q') = f(q', q')$$

и

$$0 = f(q + q', q + q') = f(q, q),$$

т. е. Q также является N-точкой. Тем самым показано, что в рассматриваемом случае каждая точка F-пространства A будет N-точкой. Но это означает, что σ является нуль-системой; отсюда и из леммы 1 (§ 2) вытекает, что f является обычной билинейной формой.

Случай 2: существует точка W, не принадлежащая P^σ и не являющаяся N-точкой. Пусть $W = Fw$. Тогда можно выбрать такую α-форму f, представляющую полярное отображение σ, что $f(w, w) = 1$; из предложения 1 (§ 3) следует, что α — инволюторный инверсный автоморфизм, а форма f — симметрическая. Так как точка W не лежит на гиперплоскости P^σ, то $f(w, P) \neq 0$ и, следовательно, существует такой элемент p, что $P = Fp$ и $f(w, p) = 1$. Отсюда, принимая во внимание симметричность формы f, мы получаем, что и $f(p, w) = 1$; в то же время, поскольку P является N-точкой, должно быть $f(p, p) = 0$. Каждая точка прямой $L = P + W$, отличная от W, имеет вид $F(p + xw)$; таким образом устанавливается взаимно однозначное соответствие между числами x из F и точками прямой L, отличными от W. Точка же $F(p + xw)$ тогда и только тогда будет N-точкой, когда

$$f(p + xw, p + xw) = x + x^\alpha + xx^\alpha = (x + 1)(x + 1)^\alpha - 1 = 0.$$

Таким образом, число N-точек прямой L равно числу решений x уравнения $(x+1)(x+1)^{\alpha}=1$ (напомним, что W не является N-точкой). Так как точка W лежит на прямой L, то $L^{\perp}$ не является N-прямой; отсюда и из условия (а) следует, что L проходит самое большее через две N-точки. Тем самым показано; что

(а*) *уравнение* $(x+1)(x+1)^{\alpha}=1$ *имеет в теле* F *самое большее два решения.*

Если мы положим $y=x+1$, то, очевидно, утверждение (а*) будет эквивалентно утверждению, что уравнение $yy^{\alpha}=1$ имеет в теле F не более двух решений y. Но легко видеть, что решениями этого уравнения будут $y=\pm 1$. Если бы это уравнение имело еще одно решение $z\neq\pm 1$, то решением его было бы также и число z^{-1}, отличное от z, $+1$ и -1; таким образом, уравнение $yy^{\alpha}=1$ обладало бы по крайней мере тремя решениями (по крайней мере четырьмя решениями, если $+1\neq -1$). Так как это невозможно, то мы доказали, что

(а**) *из* $jj^{\alpha}=1$ *следует* $j=\pm 1$.

Отсюда видно, что из условия (а) настоящего предложения следует условие (а) леммы 2; условие (б) леммы 2, которое нужно только в случае, когда характеристика тела F равна двум, следует, очевидно, из условия (б) нашего предложения. Таким образом, мы можем воспользоваться леммой 2, в силу которой $\alpha=1$, и, следовательно, полярное отображение σ представимо обычными билинейными формами. Этим предложение 3 полностью доказано.

Замечание 5. Так как утверждение (а**), как было показано, вытекает лишь из одного условия (а), то вопрос о том, не следует ли в общем случае из условия (а) предложения 3 условие (б), эквивалентен аналогичному вопросу, относящемуся к лемме 2. С другой стороны, в формулировке предложения 3 нельзя опустить предположение о существовании N-точек, как можно видеть при помощи легко строящихся примеров «положительно определенных полубилинейных форм».

Замечание 6. Пусть в линейном многообразии (F, A), ранг которого не меньше 3, существуют N-точки относительно полярного отображения σ, причем каждая прямая, содержащая более двух N-точек, является N-прямой, и характеристика тела F равна 2. При этих предположениях покажем, что

(в) *прямые, проходящие по крайней мере через две* N*-точки, являются* N*-прямыми.*

Действительно, пусть P и Q — две различные N-точки, и пусть f — некоторая полубилинейная форма, представляющая полярное отображение σ. Так как характеристика тела F равна двум, то без ограничения общности можно предположить, что f есть сим-

метрическая форма. Поэтому, если P содержится в Q^σ, то

$$0 = f(P, P) = f(P, Q) = f(Q, P) = f(Q, Q);$$

отсюда, очевидно, вытекает, что $f(P+Q, P+Q) = 0$, и, следовательно, $P+Q$ является N-прямой. Если же точка P не принадлежит гиперплоскости Q^σ, то $f(P, Q) \neq 0$; поэтому можно выбрать такие элементы p и q, что $P = Fp$, $Q = Fq$ и $f(p, q) = f(q, p) = 1$. Так как в то же время $f(p, p) = f(q, q) = 0$, то

$$f(p+q, p+q) = f(p, q) + f(q, p) = 2 = 0;$$

тем самым показано существование на прямой $P+Q$ третьей N-точки. Отсюда и из наших предположений следует, что $P+Q$ является N-прямой, чем и завершается доказательство утверждения (в).

Из утверждения (в) нетрудно вывести, что

(г) *совокупность N-точек нашего F-пространства A является подпространством.*

Некоторые свойства такого подпространства мы изучали в § 4.

Предложение 4. *Если каждая из прямых L' и L'' F-пространства A содержит по крайней мере по две N-точки, но ни одна из них не является N-прямой, то L' и L'' содержат одно и то же число N-точек.*

Доказательство. Это предложение бессодержательно, если $r(A) < 3$ или если наше полярное отображение σ является нуль-системой. Поэтому предположим, что σ не является нуль-системой и что $r(A) \geqslant 3$. Тогда, по теореме 1 (§ 3), σ представимо симметрической α-формой f, причем $\alpha^2 = 1$. Рассмотрим теперь прямую L, не являющуюся N-прямой, но содержащую две различные N-точки P и Q. Точка P не может принадлежать гиперплоскости Q^σ, ибо в противном случае, в силу леммы 3 (§ 4), L была бы N-прямой. Пусть $Q = Fq$. Тогда $f(q, q) = 0$, а $f(P, q) \neq 0$. Следовательно, существует такой элемент p, что $P = Fp$ и $f(p, q) = 1$. Отсюда, в силу симметричности формы f, $f(q, p) = 1$; в то же время, так как P является N-точкой, то $f(p, p) = 0$. Для каждой точки X прямой L, отличной от P и Q, существует, и притом только одно, такое число $x \neq 0$ из F, что $X = F(p + xq)$. Поэтому эта точка тогда и только тогда будет N-точкой, когда

$$f(p+xq, p+xq) = x + x^\alpha = 0.$$

Отсюда следует, что если обозначить через C кардинальное число таких элементов x тела F, для которых $x^\alpha = -x$ (т. е. элементов из F, кососимметрических относительно инволюторного инверсного автоморфизма α), то

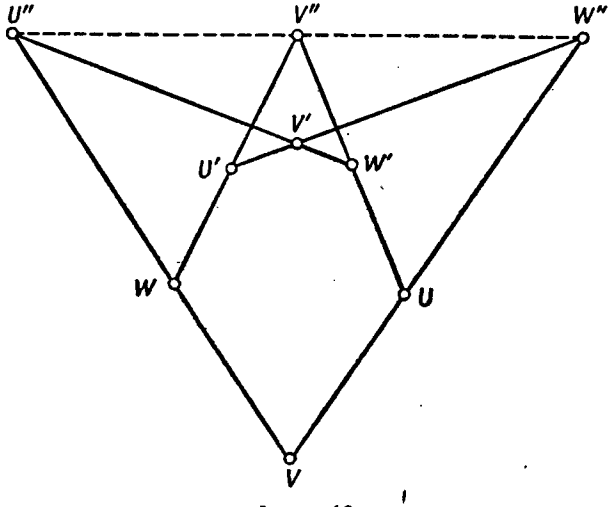
число N-точек прямой L равно $C+1$.

Полученное утверждение является несколько более сильным, чем наше предложение.

Добавление III

Теорема Паскаля

Цель нашего рассмотрения известной теоремы Паскаля вполне аналогична той цели, которую мы ставили при рассмотрении теоремы Паппа (см. гл. III, добавление II). В то время как теорема Паскаля в классической теории конических сечений справедлива без каких-либо ограничений, при нашей более общей



Фиг. 10.

точке зрения она остается справедливой, как будет показано, лишь при весьма исключительных условиях. Доказательство этой теоремы в классическом случае читатель может найти в книгах Коксетера [1] или Леви [1][1]).

Ради удобства мы в настоящем добавлении будем всюду предполагать, что линейное многообразие (F, A) является плоскостью [т. е. что $r(A) = 3$]. Это предположение весьма упростит наши рассуждения без сколько-нибудь существенного ограничения их общности, так как, в силу леммы 1 (§ 4), каждое полярное отображение индуцирует полярное отображение в произвольном неизотропном подпространстве данного линейного многообразия.

Теорема Паскаля касается определенных шестиугольников. Поэтому, прежде чем перейти к этой теореме, нам нужно немного изучить такие конфигурации. *Шестиугольником* (фиг. 10) мы назовем циклически упорядоченное множество точек $[U, V, W,$

[1]) См. также Ефимов Н. В. [1], стр. 439—441.—*Прим. перев.*

U', V', W'] нашей плоскости (F, A), удовлетворяющее условиям:

(Ш) $\begin{cases} U+V \text{ и } U'+V' \text{ являются различными прямыми, пересекающимися в некоторой точке } W''. \\ V+W \text{ и } V'+W' \text{ являются различными прямыми, пересекающимися в некоторой точке } U''. \\ W+U' \text{ и } W'+U \text{ являются различными прямыми, пересекающимися в некоторой точке } V''. \end{cases}$

Шестиугольник называется *невырожденным*, если он состоит из шести попарно различных точек (вершин) и никакие три последовательные вершины шестиугольника не коллинеарны (под последовательными вершинами мы подразумеваем точки, следующие друг за другом в смысле того циклического упорядочения, которое определено для точек шестиугольника).

Лемма 1. *Если* $[U, V, W, U', V', W']$ *– невырожденный шестиугольник, то его противоположные стороны пересекаются в трех различных точках.*

Доказательство. Противоположные стороны нашего шестиугольника пересекаются в точках U'', V'', W'' [в обозначениях условия (Ш)]. Пусть, вопреки утверждению, $U''=V''$. Тогда точка $U''=V''$ лежит на прямых $V+W$, $W+U'$, $V'+W'$ и $W'+U$. Так как V, W, U' являются последовательными вершинами шестиугольника, то они не коллинеарны; отсюда вытекает, что первые две из указанных прямых пересекаются в точке W и, следовательно, $U''=V''=W$. Но подобным же образом можно показать, что $U''=V''=W'$. Таким образом, $W=W'$, а это противоречит невырожденности нашего шестиугольника.

Полярное отображение σ плоскости называется *паскалевым*, если оно обладает следующим свойством:

(П) *Если вершины шестиугольника* $[U, V, W, U', V', W']$ *являются N-точками относительно* σ, *то противоположные стороны этого шестиугольника пересекаются в коллинеарных точках* [т. е., в обозначениях условия (Ш), точки U'', V'', W'' коллинеарны].

Связь этого свойства полярного отображения с классической теоремой Паскаля лучше всего можно заметить, если принять во внимание, что Штаудт определял коническое сечение как совокупность N-точек относительно данного полярного отображения (в нашей терминологии); следовательно, шестиугольники, вершинами которых являются N-точки, будут как раз шестиугольниками, вписанными в коническое сечение, определяемое нашим полярным отображением.

Лемма 2. *Если характеристика тела* F, *содержащего по крайней мере* 5 *элементов, отлична от* 2 *и если на плоскости* (F, A) *имеются N-точки относительно полярного отображения* σ, *то в* A *существует невырожденный шестиугольник, вершинами которого являются N-точки.*

Доказательство. Если число элементов тела F равно c, то число точек, расположенных на произвольной прямой, равно $c+1$, поскольку каждую точку прямой $Fp+Fq$, отличную от Fp, можно одним и только одним способом представить в виде $F(xp+q)$, где x — элемент тела F. Отсюда следует, что через каждую точку плоскости проходят точно $c+1$ прямых; тем самым, в силу наших предположений, через каждую точку нашей плоскости проходят по крайней мере 6 прямых. Поскольку характеристика тела F отлична от 2, можно воспользоваться предложением 2 добавления II, из которого следует, что только прямые, содержащие по одной N-точке, проходят через свой полюс. В силу этого, если прямая L, проходя через N-точку P, не совпадает с полярой P^σ, то она проходит по крайней мере еще через одну N-точку.

По нашим предположениям, существует некоторая N-точка $P(1)$. Допустим теперь, что для некоторого $i<5$ уже построены такие попарно различные N-точки $P(1), \ldots, P(i)$, что ни одна из троек последовательных точек $P(j-1)$, $P(j)$, $P(j+1)$ не коллинеарна. Так как $i<5$, то существует прямая L, проходящая через точку $P(i)$ и отличная от i прямых:

$$P(i)+P(1), \ldots, P(i)+P(i-1), P(i)^\sigma.$$

Эта прямая L содержит некоторую N-точку $P(i+1)$, отличную от $P(i)$; очевидно, что $P(i+1)$ отлична от всех ранее построенных точек и что точки $P(i-1)$, $P(i)$, $P(i+1)$ не коллинеарны. Таким образом, мы по индукции доказали существование таких пяти попарно различных N-точек $P(1), \ldots, P(5)$, что точки $P(j-1)$, $P(j)$, $P(j+1)$ $(j=2, 3, 4)$ не коллинеарны.

Существует прямая Z, проходящая через точку $P(5)$ и отличная от пяти прямых $P(5)^\sigma$, $P(5)+P(1), \ldots, P(5)+P(4)$. Эта прямая проходит также через N-точку Y, отличную от точки $P(5)$. Очевидно, что Y отлична от всех точек $P(i)$ и что три точки $P(4)$, $P(5)$, Y не коллинеарны. Но может случиться, что Y лежит на прямой $P(1)+P(2)$. В таком случае прямая $P(1)+P(2)$ содержит три N-точки; отсюда и из предложения 4 добавления II вытекает, что и прямая Z содержит по крайней мере три N-точки [1]). Таким образом, Z содержит N-точку X, отличную от Y и $P(5)$; этим показано, что всегда можно найти N-точку $P(6)$, являющуюся шестой вершиной нашего невырожденного шестиугольника.

Теорема 1. *Если характеристика тела F отлична от 2 и если на плоскости (F, A) имеются N-точки относительно полярного отображения σ, то следующие свойства полярного отображения σ эквивалентны:*

---

[1]) В начале доказательства теоремы 1 автор показывает, что на плоскости (F, A) не существует ни одной N-прямой. — *Прим. перев.*

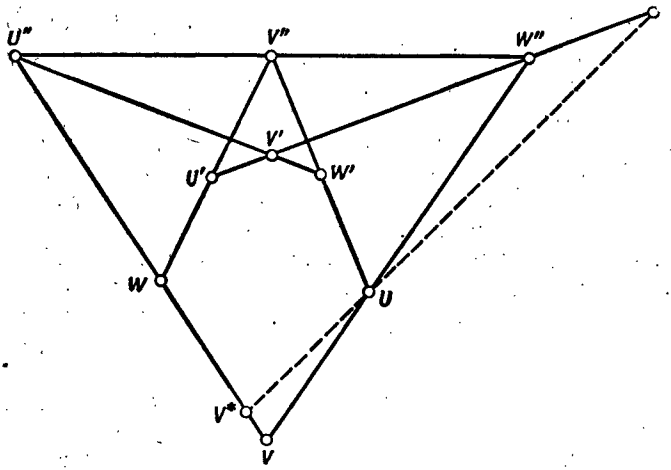
(I) *σ является паскалевым полярным отображением.*
(II) *Каждая прямая содержит не более двух N-точек.*
(III) *σ представимо обычными (симметрическими) билинейными формами.*

Доказательство. Прежде всего заметим, что на нашей плоскости не существует ни одной N-прямой. Действительно, если бы L была N-прямой, то, в силу следствия 1 (§ 4), $L \cap L^\sigma$ совпадало бы либо с 0, либо с L. Но так как L^σ есть точка, то вторая возможность отпадает. Таким образом, L должна быть неизотропной N-прямой, что невозможно, поскольку характеристика тела F отлична от 2 (следствие 2, § 4). Теперь эквивалентность свойств (II) и (III) непосредственно вытекает из предложения 3 добавления II, если принять во внимание, что характеристика тела F отлична от 2.

Если σ обладает эквивалентными между собой свойствами (II) и (III), то σ представимо обычной симметрической билинейной формой и, следовательно, F есть поле. Теперь в том, что σ является паскалевым полярным отображением, можно убедиться, пользуясь в основном теми же самыми рассуждениями, которые обычно используются при доказательстве классической теоремы Паскаля. Детали доказательства мы оставляем в качестве упражнения читателю. Таким образом, свойство (I) является следствием как свойства (II), так и свойства (III).

Пусть теперь справедливо свойство (I). Если тело F содержит меньше пяти элементов, то число элементов тела F равно 3, поскольку его характеристика отлична от 2. В этом случае тело состоит лишь из целых кратных единицы и, следовательно, единственным автоморфизмом, а также единственным инверсным автоморфизмом этого тела будет тождественный автоморфизм. Но тогда каждая полубилинейная форма будет обычной билинейной формой; таким образом, в этом случае то, что свойство (III) следует из свойства (I), очевидно. Поэтому предположим, что тело F содержит по крайней мере 5 элементов. Тогда из нашего предположения о существовании N-точек и леммы 2 вытекает существование невырожденного шестиугольника $[U, V, W, U', V', W']$, вершинами которого являются N-точки. Противоположные стороны этого шестиугольника пересекаются в точках U'', V'', W'' [использованы обозначения условия (Ш)]; по лемме 1, эти точки попарно различны, а из свойства (I) следует, что они коллинеарны. Таким образом, $T = U'' + V'' = V'' + W'' = W'' + U''$ является прямой. Поскольку как противоположные, так и смежные стороны нашего шестиугольника попарно различны (все шесть сторон шестиугольника попарно различны), самое большее одна из сторон нашего шестиугольника совпадает с прямой T; поэтому без ограничения общности можно предположить, что T отлична от сторон $U + V$

и $U'+V'$. В таком случае прямая T пересекается с этими сторонами в одной точке W''. Так как смежные стороны различны, то без ограничения общности можно, кроме того, предположить, что вершина U не лежит на стороне $U'+V'$ и, следовательно, $U \neq W''$. Теперь допустим, вопреки утверждению, что существует прямая, содержащая более двух N-точек. Тогда прямая $V+W$, проходя



Фиг. 11.

через две N-точки V и W, в силу предложения 4 добавления II, должна пройти и через третью N-точку V^* (фиг. 11). Легко проверить, что $[U, V^*, W, U', V', W']$ является шестиугольником, вершинами которого будут N-точки. Поскольку $V^*+W=V+W$, противоположные стороны этого шестиугольника пересекаются в точках $(U+V^*)\cap(U'+V')$, U'', V''. В силу свойства (I), эти точки коллинеарны; следовательно, прямые $U+V^*$, $U'+V'$, $U''+V''=T$ пересекаются в одной точке, которой непременно должна быть точка W''. Таким образом, прямые $U+V$ и $U+V^*$ обе проходят через точку W'', и так как $U \neq W''$, то $U+V=U+W''=U+V^*$. Отсюда вытекает, что V^* является общей точкой двух различных прямых $U+V$ и $V+W$ и, следовательно, $V=V^*$, что невозможно. Полученное противоречие показывает, что при выполнении свойства (I) выполняется и свойство (II); тем самым теорема 1 полностью доказана.

В качестве хорошего упражнения мы предлагаем читателю найти чисто алгебраическое доказательство того, что из свойства (I) следует свойство (II), вместо приведенного нами синтетического доказательства этого утверждения.

Замечание 1. Вопрос о том, в какой степени по существу необходимо предположение, что характеристика тела F отлична

от 2, еще полностью не исследован. Тем не менее, если F есть поле характеристики 2, то легко построить симметрическую билинейную форму над плоскостью (F, A), представляющую такое полярное отображение σ, что все N-точки плоскости образуют прямую (см., например, доказательство предложения 1, § 4). Это полярное отображение σ обладает свойством (III), но не обладает свойством (II); очевидно, что в этом случае не существуют шестиугольники, вершинами которых были бы N-точки, и поэтому не верна лемма 2.

Теорема 2. *Если характеристика тела F отлична от 2, то каждое полярное отображение плоскости (F, A) тогда и только тогда является паскалевым, когда не существует инволюторного инверсного автоморфизма тела F, отличного от тождественного.*

Доказательство. Если тело F не обладает ни одним инволюторным инверсным автоморфизмом, кроме, быть может, тождественного, то каждое полярное отображение плоскости (F, A), если оно существует, представимо, в силу предложения 1 (§ 1), обычной билинейной формой. Отсюда и из теоремы 1 следует, что каждое полярное отображение плоскости (F, A) будет паскалевым. Обратно, пусть каждое полярное отображение плоскости (F, A) является паскалевым. Рассмотрим произвольный инволюторный инверсный автоморфизм α тела F. Если b_1, b_2, b_3 — базис плоскости A, то можно следующим образом определить α-форму f над A:

$$f\left(\sum_{i=1}^{3} x_i b_i, \sum_{i=1}^{3} y_i b_i\right) = x_1 y_1^{\alpha} + x_2 y_2^{\alpha} - x_3 y_3^{\alpha}.$$

Легко проверить, что форма f является α-симметрической и что f представляет некоторое полярное отображение σ (см. предложение 2, § 1, и лемму 1, § 3). Относительно этого полярного отображения существуют N-точки, например точка $F(b_1 - b_3)$; следовательно, приняв во внимание, что, по предположению, σ является паскалевым полярным отображением, мы из теоремы 1 выведем, что $\alpha = 1$. Таким образом, теорема 2 полностью доказана.

Замечание 2. Из теоремы 2 (§ 3) вытекает, что если тело F не обладает ни одним инволюторным инверсным автоморфизмом, то плоскость (F, A) не обладает полярными отображениями. Таким образом, наша теорема тривиально справедлива при отсутствии инволюторных инверсных автоморфизмов тела F. Если же к условию теоремы добавить предположение о существовании инволюторных инверсных автоморфизмов, то из условия, что тождественный автоморфизм является единственным инволюторным инверсным автоморфизмом тела F, следует, что F будет полем.

Замечание 3. С полным правом можно сказать, что в плоскости (F, A) выполняется теорема Паскаля, если каждое полярное

отображение этой плоскости является паскалевым. Таким образом, теорема 2 характеризует те плоскости, в которых справедлива теорема Паскаля.

Замечание 4. В процессе разыскания плоскостей, для которых справедлива теорема Паскаля, мы выделили класс полей F характеристики, отличной от 2, обладающих следующим свойством:

(*) *Поле F не имеет автоморфизмов порядка 2.*

Простым примером поля, обладающего свойством (*), является поле действительных чисел; простым примером поля, в котором условие (*) не выполняется, является поле комплексных чисел. Другие примеры полей, обладающих свойством (*), можно получить, используя некоторые элементарные результаты из теории Галуа; эти результаты изложены в книгах Артина [1], Биркгофа и Мак-Лейна [1], Ван-дер-Вардена [2] и др. Пусть F есть поле и α—автоморфизм поля F порядка 2. Обозначим через D совокупность таких элементов d из F, для которых $d^\alpha = d$. D является подполем поля F, и степень расширения поля F над D равна 2. Обратно, каждому подполю S поля F, над которым F является расширением 2-й степени, соответствует такой автоморфизм 2-го порядка. Отсюда видно, что условие (*) эквивалентно следующему условию:

(**) *Поле F не является расширением 2-й степени ни над одним из своих подполей.*

Например, если поле F является расширением нечетной степени поля рациональных чисел (или любого другого простого поля), то F непременно обладает свойством (**). Небезынтересен следующий критерий совсем иного типа, поскольку он часто оказывается полезным в приложениях.

Поле F обладает свойством (**), *если оно удовлетворяет следующим двум условиям:*

(а) *Из* $\sum_{i=1}^{n} x_i^2 = 0$ *следует* $x_1 = \ldots = x_n = 0$.

(б) *Если x — отличный от 0 элемент поля F, то либо x, либо $-x$ является квадратом элемента из F.*

[Поля, обладающие свойством (а), называются *формально действительными*; поля, в которых выполнены свойства (а) и (б), называются *евклидовыми*.]

Доказательство. Пусть в поле F выполняются условия (а) и (б), и пусть, вопреки утверждению, в F существует такое подполе D, что F является расширением 2-й степени над D. В таком случае поле F можно получить, присоединяя к D такой элемент e, что $e^2 = d$ содержится в D. Так как $F \neq D$, то $e \neq 0$; поскольку и $(-e)^2 = d$, без ограничения общности можно предположить, что e является квадратом некоторого элемента b из F— здесь мы пользуемся условием (б). Элемент b, как и каждый

элемент поля F, можно представить в виде $b = b' + b''e$, где b' и b'' — элементы из D; отсюда следует, что

$$e = b^2 = (b' + b''e)^2 = b'^2 + b''^2 d + 2b'b''e.$$

Таким образом, $2b'b'' = 1$ и $0 = b'^2 + b''^2 d = b'^2 + (b''e)^2$. Применяя теперь ко второму равенству условие (а), мы находим, что $b' = b''e = 0$. Но это противоречит равенству $2b'b'' = 1$; полученное противоречие доказывает справедливость свойства (**).

§ 5. Группа полярного отображения

На протяжении всего этого параграфа мы будем предполагать, что ранг F-пространства A не меньше 3. При этом ограничении каждое автодуальное отображение представимо полубилинейной формой (предложение 1, § 1) и каждое проективное отображение индуцируется полулинейным преобразованием (первая основная теорема проективной геометрии, гл. III, § 1).

Пусть δ — автодуальное отображение и π — автопроективное отображение F-пространства A; тогда π называется *δ-допустимым проективным отображением*, если $\pi\delta = \delta\pi$. Это условие означает, что равенство $U^{\pi\delta} = U^{\delta\pi}$ справедливо для каждого подпространства U F-пространства A. Совокупность всех δ-допустимых проективных отображений является, очевидно, группой. Эта группа в первую очередь имеет право на название «группа дуального отображения δ». Существуют, однако, и многие другие группы, которые, как будет показано, столь же важны.

Предложение 1. *Если дуальное отображение δ представимо полубилинейной формой f, то полулинейное преобразование σ F-пространства A тогда и только тогда индуцирует δ-допустимое проективное отображение, когда в F существует такое число $c \neq 0$, что*

$$f(x^\sigma, y^\sigma) = f(x, y)^\sigma c \quad \text{для любых } x, y \text{ из } A.$$

Доказательство. Предположим, что наше условие справедливо. Если M есть подпространство F-пространства A, то элемент x тогда и только тогда принадлежит M^δ, когда $f(x, M) = 0$. Это условие эквивалентно тому, что $0 = f(x, M)^\sigma c = f(x^\sigma, M^\sigma)$. Таким образом, x тогда и только тогда принадлежит M^δ, когда x^σ принадлежит $(M^\sigma)^\delta$. Отсюда следует, что $M^{\delta\sigma} = M^{\sigma\delta}$, и этим показано, что проективное отображение, индуцированное полулинейным преобразованием σ, является δ-допустимым.

Обратно, пусть σ индуцирует δ-допустимое проективное отображение. Определим функцию

$$g(x, y) = f(x^\sigma, y^\sigma)^{\sigma^{-1}} \quad \text{для любых } x, y \text{ из } A.$$

Очевидно, что функция $g(x, y)$ аддитивна относительно x и y. Если теперь t — число из F, то

$$g(tx, y) = f([tx]^\sigma, y^\sigma)^{\sigma^{-1}} = f(t^\sigma x^\sigma, y^\sigma)^{\sigma^{-1}} = [t^\sigma f(x^\sigma, y^\sigma)]^{\sigma^{-1}} = tg(x, y).$$

Существует такой инверсный автоморфизм α тела F, что f является α-формой. Принимая это во внимание, мы получаем

$$g(x, ty) = f(x^\sigma, [ty]^\sigma)^{\sigma^{-1}} = f(x^\sigma, t^\sigma y^\sigma)^{\sigma^{-1}} = \\ = [f(x^\sigma, y^\sigma) t^{\sigma\alpha}]^{\sigma^{-1}} = g(x, y) t^{\sigma\alpha\sigma^{-1}}.$$

Так как $\sigma\alpha\sigma^{-1} = \beta$ также будет инверсным автоморфизмом тела F, то тем самым показано, что $g(x, y)$ является β-формой.

Если M есть подпространство F-пространства A, то элемент x тогда и только тогда содержится в M^δ, когда $f(x, M) = 0$. Другим необходимым и достаточным условием того, что x содержится в M^δ, является требование, чтобы x^σ содержался в $M^{\delta\sigma}$. Но σ индуцирует δ-допустимое проективное отображение; поэтому $M^{\delta\sigma} = M^{\sigma\delta}$. Таким образом, показано, что $f(x, M) = 0$ тогда и только тогда, когда x^σ содержится в $M^{\sigma\delta}$; последнее же утверждение эквивалентно тому, что $f(x^\sigma, M^\sigma) = 0$. Поскольку это равенство справедливо тогда и только тогда, когда $0 = f(x^\sigma, M^\sigma)^{\sigma^{-1}} = g(x, M)$, мы, наконец, показали, что

$$f(x, M) = 0 \text{ тогда и только тогда, когда } g(x, M) = 0;$$

отсюда следует, что полубилинейные формы $f(x, y)$ и $g(x, y)$ представляют одно и то же дуальное отображение δ. Поэтому, в силу предложения 3 (§ 1), в F существует такое число $z \neq 0$, что $g(x, y) = f(x, y) z$. Таким образом,

$$f(x, y) z = g(x, y) = f(x^\sigma, y^\sigma)^{\sigma^{-1}}, \text{ откуда } f(x^\sigma, y^\sigma) = f(x, y)^\sigma z^\sigma;$$

тем самым необходимость нашего условия доказана.

Напомним, что отображение σ является линейным преобразованием, если оно представляет собой автоморфизм аддитивной группы A, удовлетворяющий условию $(xy)^\sigma = xy^\sigma$ для любых x из F и y из A. Если, кроме того, $\sigma^2 = 1$, то мы будем называть σ *инволюцией* (или *инволюторным линейным преобразованием*).

Лемма 1. *Пусть σ есть инволюция F-пространства A. Обозначим через $J^+(\sigma)$ множество всех таких элементов x из A, что $x^\sigma = x$; через $J^-(\sigma)$ обозначим множество всех таких элементов x из A, что $x^\sigma = -x$. $J^+(\sigma)$ и $J^-(\sigma)$ являются подпространствами F-пространства A, и если характеристика тела F отлична от 2, то $A = J^+(\sigma) + J^-(\sigma)$.*

Это утверждение доказывается очень просто; нужно только принять во внимание, что для каждого x из A элементы $x + x^\sigma$ и $x - x^\sigma$ содержатся соответственно в $J^+(\sigma)$ и $J^-(\sigma)$.

Лемма 2. *Если характеристика тела F отлична от 2 и если полярное отображение π представимо полубилинейной формой $f(x, y)$, а σ является инволюцией, то:*

(а) *σ тогда и только тогда индуцирует π-допустимое проективное отображение, когда $f(x, y) = e f(x^\sigma, y^\sigma)$ для любых x и y из A, причем $e = \pm 1$.*

(б) *Тогда и только тогда $f(x, y) = f(x^\sigma, y^\sigma)$ для любых x и y из A, когда*

$$J^+(\sigma)^\pi = J^-(\sigma) \quad и \quad J^-(\sigma)^\pi = J^+(\sigma).$$

(в) *Тогда и только тогда $f(x, y) = -f(x^\sigma, y^\sigma)$ для любых x и y из A, когда*

$$J^+(\sigma)^\pi = J^+(\sigma) \quad и \quad J^-(\sigma)^\pi = J^-(\sigma).$$

Доказательство. Из предложения 1 следует, что условие, сформулированное в утверждении (а), является достаточным. Обратно, если инволюция σ индуцирует π-допустимое проективное отображение, то, в силу предложения 1, в F существует такое число $c \neq 0$, что $f(x^\sigma, y^\sigma) = f(x, y)\, c$ для любых x и y, поскольку σ — линейное преобразование. Но $\sigma^2 = 1$; поэтому

$$f(x, y) = f(x^{\sigma^2}, y^{\sigma^2}) = f(x^\sigma, y^\sigma)\, c = f(x, y)\, c^2.$$

Так как форма $f(x, y)$ не равна тождественно 0, то из полученного равенства следует, что $c^2 = 1$, откуда $c = \pm 1$; тем самым утверждение (а) доказано.

Пусть теперь $J^+(\sigma)^\pi = J^-(\sigma)$ и $J^-(\sigma)^\pi = J^+(\sigma)$. Тогда для любых x из $J^+(\sigma)$ и y из $J^-(\sigma)$ будет $f(x, y) = f(y, x) = 0$. Если теперь u и v — произвольные элементы F-пространства A, то, по лемме 1, $u = u' + u''$, $v = v' + v''$, где $u', v' \in J^+(\sigma)$ и $u'', v'' \in J^-(\sigma)$. Поэтому

$$f(u^\sigma, v^\sigma) = f(u' - u'', v' - v'') = f(u', v') + f(u'', v'') = f(u, v).$$

Обратно, пусть $f(x^\sigma, y^\sigma) = f(x, y)$ для любых x и y из A. Тогда, если элемент x содержится в $J^+(\sigma)$, а элемент y — в $J^-(\sigma)$, то

$$f(x, y) = f(x^\sigma, y^\sigma) = f(x, -y) = -f(x, y);$$

отсюда следует, что $f(x, y) = 0$, поскольку характеристика тела F отлична от 2. Таким образом, $J^+(\sigma) \leqslant J^-(\sigma)^\pi$. Но из леммы 1 и следствия 1 (§ 1) вытекает, что $r[J^+(\sigma)] = r[J^-(\sigma)^\pi]$. Поэтому $J^+(\sigma) = J^-(\sigma)^\pi$ и, следовательно, $J^-(\sigma) = J^+(\sigma)^\pi$. Тем самым утверждение (б) доказано.

Пусть теперь $J^+(\sigma)^\pi = J^+(\sigma)$ и $J^-(\sigma)^\pi = J^-(\sigma)$. Если x и y — произвольные элементы F-пространства A, то, по лемме 1, $x = x' + x''$, $y = y' + y''$, где $x', y' \in J^+(\sigma)$ и $x'', y'' \in J^-(\sigma)$. Так как

$f(x', y') = f(x'', y'') = 0$, то

$$f(x^\sigma, y^\sigma) = f(x' - x'', y' - y'') = -f(x'', y') - f(x', y'') = \\ = -[f(x', y') + f(x', y'') + f(x'', y') + f(x'', y'')] = -f(x, y).$$

Обратно, если равенство $f(x^\sigma, y^\sigma) = -f(x, y)$ справедливо для любых x и y из A и если элементы u, v оба содержатся в $J^+(\sigma)$, то

$$-f(u, v) = f(u^\sigma, v^\sigma) = f(u, v)$$

и, следовательно, $f(u, v) = 0$, так как характеристика тела F отлична от 2. Подобным же образом можно показать, что $f(u, v) = 0$, если элементы u, v оба содержатся в $J^-(\sigma)$. Таким образом, мы установили, что

$$J^+(\sigma) \leqslant J^+(\sigma)^\pi \quad \text{и} \quad J^-(\sigma) \leqslant J^-(\sigma)^\pi.$$

Отсюда, а также из леммы 1 и следствия 1 (§ 1) вытекает, что

$$r([J^+(\sigma)] \leqslant r[J^+(\sigma)^\pi] = r[J^-(\sigma)] \leqslant r[J^-(\sigma)^\pi] = r[J^+(\sigma)],$$

т. е. все эти четыре ранга равны друг другу. Отсюда и из полученных выше включений следуют равенства $J^+(\sigma) = J^+(\sigma)^\pi$, $J^-(\sigma) = J^-(\sigma)^\pi$, и этим утверждение (в) полностью доказано.

Замечание 1. Заметим, что в случае (в), в силу леммы 1 и результатов, полученных в конце доказательства леммы 2,

$$r[J^+(\sigma)] = r[J^-(\sigma)] = \tfrac{1}{2} r(A),$$

так что $r(A)/2$ является индексом нашего полярного отображения (в смысле § 4).

Если инволюция σ, индуцирующая такое π-допустимое проективное отображение, удовлетворяет условию

$$f(x^\sigma, y^\sigma) = f(x, y) \text{ для любых } x \text{ и } y \text{ из } A,$$

где f — некоторая полубилинейная форма, представляющая полярное отображение π, то то же самое равенство справедливо, очевидно, для любой полубилинейной формы, представляющей π; в этом случае мы будем называть σ *π-допустимой инволюцией первого рода*. Все другие инволюции, индуцирующие π-допустимые проективные отображения, будут называться *π-допустимыми инволюциями второго рода*. Группу линейных преобразований, порождаемую π-допустимыми инволюциями первого рода, обозначим через $\Gamma(\pi)$. Каждый элемент группы $\Gamma(\pi)$ является линейным преобразованием F-пространства A, индуцирующим π-допустимое проективное отображение; если $f(x, y)$ — некоторая полубилинейная форма, представляющая полярное отображение π, то $f(x^\sigma, y^\sigma) = f(x, y)$ для любых x, y из A и произвольного σ из $\Gamma(\pi)$.

Из последнего замечания следует, что $\Gamma(\pi)$ не содержит π-допустимых инволюций второго рода, если только, конечно, харак-

теристика тела F отлична от 2. Отметим, кроме того, что из замечания 1 видно, насколько редко встречаются π-допустимые инволюции второго рода; в то же время следующее утверждение показывает, как много существует π-допустимых инволюций первого рода.

Следствие 1. *Если характеристика тела F отлична от 2, полулинейная форма $f(x, y)$ представляет полярное отображение π и U есть подпространство F-пространства A, то U тогда и только тогда неизотропно, когда существует такая π-допустимая инволюция σ первого рода, что $U = J^+(\sigma)$.*

Доказательство. Достаточность нашего условия непосредственно следует из равенства

$$U \cap U^\pi = J^+(\sigma) \cap J^-(\sigma) = 0,$$

которое справедливо в силу того, что характеристика основного тела отлична от 2.

Обратно, пусть $U \cap U^\pi = 0$. Тогда, в силу следствия 2 (§ 1), $A = U \dotplus U^\pi$. Поэтому можно построить такое линейное преобразование σ F-пространства A, при котором $x^\sigma = x$ для x из U и $x^\sigma = -x$ для x из U^π. Очевидно, что σ является инволюцией и что $U = J^+(\sigma)$, $U^\pi = J^-(\sigma)$; отсюда и из утверждений (а), (б) леммы 2 следует, что σ является π-допустимой инволюцией первого рода.

Замечание 2. Вместо равенства $U = J^+(\sigma)$ можно было бы требовать выполнение равенства $U = J^-(\sigma)$.

Следующая теорема показывает, что полярные отображения однозначно определяются своими группами.

Теорема 1. *Если характеристика тела F отлична от 2, то следующие свойства полярных отображений π' и π'' F-пространства A, ранг которого $r(A) > 2$, эквивалентны:*

(I) $\pi' = \pi''$.

(II) *Множества π'-допустимых и π''-допустимых проективных отображений совпадают.*

(III) *Множества π'-допустимых и π''-допустимых коллинеаций совпадают.*

(IV) $\Gamma(\pi') = \Gamma(\pi'')$.

Доказательство. Очевидно, что из свойства (I) следует свойство (II) и что из свойства (II) следует свойство (III). Пусть теперь справедливо свойство (III). Обозначим через Θ группу линейных преобразований, индуцирующих π'-допустимые коллинеации. Согласно свойству (III), эта группа совпадает с группой всех линейных преобразований, индуцирующих π''-допустимые коллинеации. Отсюда и из определения группы Γ следует, что Θ содержит обе группы $\Gamma(\pi')$ и $\Gamma(\pi'')$. Докажем теперь, что

(IV. а) если σ является π'-допустимой инволюцией первого рода, то σ будет также π''-допустимой инволюцией первого рода.

Действительно, если утверждение (IV. а) не справедливо, то σ должна быть π''-допустимой инволюцией второго рода, ибо, по свойству (III), σ индуцирует π''-допустимую коллинеацию. Следовательно,

$$J^+(\sigma) = J^+(\sigma)^{\pi''} = J^-(\sigma)^{\pi'}, \quad J^-(\sigma) = J^-(\sigma)^{\pi''} = J^+(\sigma)^{\pi'};$$

отсюда, в силу замечания 1,

$$k = r[J^+(\sigma)] = r[J^-(\sigma)] = \frac{1}{2} r(A),$$

и поэтому $1 < k$; из леммы же 1 вытекает, что $A = J^+(\sigma) \dotplus J^-(\sigma)$.

В силу следствия 1, $J^+(\sigma)$ есть неизотропное подпространство относительно π'. Так как характеристика основного тела отлична от 2 и ранг подпространства $J^+(\sigma)$ больше 1, то, пользуясь следствием 2 (§ 4), мы получаем, что либо π' является нуль-системой, либо $J^+(\sigma)$ не обладает свойством (N) относительно π'.

Случай 1: $J^+(\sigma)$ не обладает свойством (N) относительно π'. В этом случае существует такая точка P, содержащаяся в $J^+(\sigma)$, что $P \cap P^{\pi'} = 0$. Таким образом, P есть неизотропная относительно π' точка; поэтому, в силу следствия 1, существует такая π'-допустимая инволюция σ', что $P = J^+(\sigma')$, $P^{\pi'} = J^-(\sigma')$. Очевидно, что σ' содержится в Θ и, следовательно, является и π''-допустимой инволюцией. Поскольку подпространство $J^+(\sigma)$ строго изотропно относительно π'', точка P обладает свойством (N) относительно π'', и поэтому σ' не может быть π''-допустимой инволюцией первого рода (следствие 1). Но так как $r(P) = 1 < r(A)/2$, то из леммы 2 и замечания 1 следует, что σ' не может быть и π''-допустимой инволюцией второго рода. Таким образом, мы пришли к противоречию.

Случай 2: $J^+(\sigma)$ является N-подпространством относительно π'. В этом случае, как было уже замечено, π' будет нуль-системой. Поэтому, в силу утверждений (б) и (в) леммы 1 (§ 2), π' представимо некоторой (обычной) кососимметрической билинейной формой $g(x, y)$; в то же время из предложения 1 (§ 2) вытекает, что неизотропное подпространство $J^+(\sigma)$ содержит неизотропное подпространство U ранга 2, обладающее таким базисом a, b, что $g(a, b) = 1 = -g(b, a)$. Обозначим через τ однозначно определенное линейное преобразование F-пространства A, удовлетворяющее следующим условиям:

$$a^\tau = b, \quad b^\tau = -a, \quad x^\tau = x \text{ для } x \text{ из } U^{\pi'}.$$

Так как U — неизотропное подпространство, то, в силу следствия 2 (§ 1), $A = U \dotplus U^{\pi'}$; поэтому каждый элемент x из A можно однозначно представить в виде $x = x'a + x''b + x^0$, где $x', x'' \in F$ и $x^0 \in U^{\pi'}$.

Отсюда следует, что

$$g(x, y) = g(x'a + x''b + x^0, y'a + y''b + y^0) = x'y'' - x''y' + g(x^0, y^0),$$

поскольку $g(U, U^{\pi'}) = g(U^{\pi'}, U) = 0$, $g(a, a) = g(b, b) = 0$. Поэтому

$$g(x^\tau, y) = g(-x''a + x'b + x^0, -y''a + y'b + y^0) =$$
$$= -x''y' + x'y'' + g(x^0, y^0) = g(x, y);$$

таким образом, в силу предложения 1, τ индуцирует π'-допустимую коллинеацию. Следовательно, τ содержится в группе Θ, и поэтому коллинеация, индуцированная линейным преобразованием τ, будет и π''-допустимой. Теперь, если представить π'' некоторой полубилинейной формой $h(x, y)$ (предложение 1, § 1), то, в силу предложения 1, в теле F существует такое число $c \neq 0$, что $h(x^\tau, y^\tau) = h(x, y)c$ для любых x и y из A.

Так как точки Fa и Fb различны, то и гиперплоскости $(Fa)^{\pi''}$ и $(Fb)^{\pi''}$ различны. Из $Fa \leqslant J^+(\sigma) = J^+(\sigma)^{\pi''}$ вытекает, что $J^+(\sigma) \leqslant (Fa)^{\pi''}$; из тех же соображений видно, что $J^+(\sigma) \leqslant (Fb)^{\pi''}$. Поскольку $U \leqslant J^+(\sigma)$, мы имеем $J^-(\sigma) = J^+(\sigma)^{\pi'} \leqslant U^{\pi'}$. Так как $(Fa)^{\pi''}$ и $(Fb)^{\pi''}$ — различные гиперплоскости и, следовательно, ни одна из них не содержится в другой, то в $(Fa)^{\pi''}$ существует элемент z, не принадлежащий $(Fb)^{\pi''}$. В силу леммы 1, $A = J^+(\sigma) + J^-(\sigma)$; поэтому $z = w + u$, где $w \in J^+(\sigma)$ и $u \in J^-(\sigma) \leqslant U^{\pi'}$. Так как $J^+(\sigma) \leqslant (Fa)^{\pi''} \cap (Fb)^{\pi''}$, то w содержится в $(Fa)^{\pi''} \cap (Fb)^{\pi''}$, и поэтому элемент u содержится в $(Fa)^{\pi''}$, но не содержится в $(Fb)^{\pi''}$. Таким образом, $h(u, a) = h(a, u) = 0$, и в то же время ни одно из значений $h(u, b)$, $h(b, u)$ не равно 0 [см. лемму 1 (S), § 3]. Теперь из наших рассуждений легко следует равенство

$$h(b, u)c = h(b^\tau, u^\tau) = h(-a, u) = 0,$$

которое приводит нас к противоречию, поскольку оба числа c и $h(b, u)$ отличны от 0. Тем самым утверждение (IV. а) полностью доказано.

Аналогичными рассуждениями можно показать, что справедливо утверждение, обратное утверждению (IV. а); следовательно, σ тогда и только тогда является π'-допустимой инволюцией первого рода, когда σ является π''-допустимой инволюцией первого рода. Из этого утверждения вытекает, очевидно, равенство групп $\Gamma(\pi')$ и $\Gamma(\pi'')$; таким образом, показано, что свойство (IV) следует из свойства (III).

Пусть теперь справедливо свойство (IV). Если U есть неизотропное относительно π' подпространство F-пространства A, то, в силу следствия 1, существует такая π'-допустимая инволюция σ первого рода, что $U = J^+(\sigma)$. Но ввиду справедливости свойства (IV), σ содержится и в группе $\Gamma(\pi'')$. Поскольку (как было отмечено

выше) $\Gamma(\pi'')$ не содержит инволюций второго рода, σ является π''-допустимой инволюцией первого рода. Отсюда и из утверждений (а), (б) леммы 2 следует, что $U^{\pi''} = J^{-}(\sigma) = U^{\pi'}$. Аналогичный результат справедлив также и для подпространств V, неизотропных относительно полярного отображения π''; таким образом, мы показали:

(I. а) Подпространство U тогда и только тогда неизотропно относительно π', когда оно неизотропно относительно π''; если подпространство U неизотропно относительно π' и π'', то $U^{\pi'} = U^{\pi''}$.

Далее нам понадобится следующая лемма.

(1. а) *Если π — полярное отображение F-пространства A и если P — точка этого пространства, обладающая свойством (N), то P является точкой пересечения двух неизотропных прямых.*

Доказательство леммы (1.а). По предположению, $P \leqslant P^{\pi}$. Далее, так как P^{π} есть гиперплоскость и $r(A) > 2$, то существуют по крайней мере две различные прямые L' и L'', проходящие через точку P и не содержащиеся в P^{π}. Очевидно, что $L' \cap P^{\pi} = P$. Так как L' не содержится в P^{π}, то P не принадлежит подпространству L'^{π}; в то же время, так как P является точкой прямой L', то $L'^{\pi} \leqslant P^{\pi}$. Отсюда следует, что

$$L' \cap L'^{\pi} = L' \cap P^{\pi} \cap L'^{\pi} = P \cap L'^{\pi} = 0;$$

точно так же можно показать, что и прямая L'' неизотропна. Тем самым лемма (1.а) доказана.

Возвращаемся к доказательству нашей теоремы; его мы проведем, используя лишь утверждение (1.а) [как было показано, это утверждение следует из свойства (IV)]. Если P — точка F-пространства A, то из (1.а) вытекает, что P тогда и только тогда обладает свойством (N) относительно π', когда она обладает свойством (N) относительно π''. Далее, если точка P не обладает свойством (N), то из того же утверждения (1.а) следует, что $P^{\pi'} = P^{\pi''}$. Если же P обладает свойством (N) (относительно π' и π''), то, по лемме (1.а), $P = L' \cap L''$, где L' и L'' — неизотропные относительно π' прямые. Вновь используя утверждение (1.а), мы получаем, что прямые L' и L'' неизотропны и относительно π'' и что $L'^{\pi'} = L'^{\pi''}$, $L''^{\pi'} = L''^{\pi''}$. Следовательно,

$$P^{\pi'} = (L' \cap L'')^{\pi'} = L'^{\pi'} + L''^{\pi'} = L'^{\pi''} + L''^{\pi''} = (L' \cap L'')^{\pi''} = P^{\pi''}.$$

Таким образом, доказано, что

$$P^{\pi'} = P^{\pi''} \text{ для каждой точки } P \text{ } F\text{-пространства } A.$$

Но каждое подпространство S линейного многообразия (F, A) есть сумма конечного числа точек; поэтому

$$S^{\pi'} = \left[\sum_{i=1}^{s} P_i\right]^{\pi'} = P_1^{\pi'} \cap \ldots \cap P_s^{\pi'} =$$

$$= P_1^{\pi''} \cap \ldots \cap P_s^{\pi''} = \left[\sum_{i=1}^{s} P_i\right]^{\pi''} = S^{\pi''},$$

откуда $\pi' = \pi''$. Таким образом, свойство (I) следует из (I.а), и этим теорема полностью доказана.

Укажем следующее важное применение этой теоремы. Пусть $f(x, y)$ — полубилинейная форма над A; мы будем говорить, что преобразование τ F-пространства A *сохраняет форму* $f(x, y)$, если $f(x^\tau, y^\tau) = f(x, y)$ для любых x и y из A. Отметим, что π-допустимая инволюция первого рода сохраняет формы, представляющие полярное отображение π; в то же время π-допустимые инволюции второго рода этим свойством не обладают. Заметим, кроме того, что полулинейное преобразование τ, сохраняющее полубилинейную форму $f(x, y)$, не равную тождественно 0, является линейным.

Следствие 2. *Если характеристика тела F отлична от 2 и если полубилинейные формы f и g над F-пространством A $[r(A) > 2]$ представляют полярные отображения, то f и g тогда и только тогда сохраняются одними и теми же линейными преобразованиями, когда в F существует такое число $c \neq 0$, что $f(x, y) = g(x, y)c$ для любых x и y из A; это эквивалентно тому, что f и g представляют одно и то же полярное отображение.*

Доказательство. Достаточность нашего условия очевидна, и нам нужно только доказать его необходимость. Для этого предположим, что одни и те же линейные преобразования сохраняют полубилинейные формы f и g. Обозначим через π' и π'' полярные отображения, представимые соответственно формами f и g. Из нашего предположения вытекает, что одни и те же коллинеации будут π'- и π''-допустимыми. Отсюда, по теореме 1, $\pi' = \pi''$. Таким образом, f и g представляют одно и то же полярное отображение; поэтому, в силу предложения 3 (§ 1), в теле F существует такое число $c \neq 0$, что $f(x, y) = g(x, y)c$.

Замечание 3. Интересную геометрическую интерпретацию последнего результата можно получить следующим образом. Рассматриваем A как $r(A)$-мерное векторное пространство над телом F. Полубилинейной форме $f(x, y)$, представляющей полярное отображение, придадим следующий смысл: $f(x, x)$ есть «мера длины вектора x» [точнее, $f(x, x)$ является «квадратом длины» вектора x]; в то же время значение $f(x, y)$ представляет собой некоторый способ измерения «угла между векторами x и y». Линейные преобразования, сохраняющие форму f, составляют «группу

геометрии, определенной в векторном пространстве A полубилинейной формой f». При такой терминологии следствие 2 утверждает, что геометрия и ее группа однозначно определяют друг друга, если пренебречь возможным изменением «единицы измерения». Векторы x и y ортогональны друг другу в нашей f-геометрии [1]), если $f(x, y) = 0$. Отношение ортогональности между векторами определяет отношение ортогональности между подпространствами, которое в сущности является не чем иным, как полярным отображением, представимым полубилинейной формой f. Из предложения 3 (§ 1) следует, что это полярное отображение, а значит, и наше отношение ортогональности определяют полубилинейную форму однозначно с точностью до постоянного множителя. Таким образом, мы видим, что следующие понятия по существу тождественны: f-геометрия, отношение f-ортогональности и группы, определяемые каждым из этих понятий. Так как $f(x, x)$ может равняться 0 для каждого вектора x из A, то «квадрат длины» векторов не всегда полностью определяет f-геометрию. Но если мы исключим случай, когда f представляет нуль-систему, то, как мы сейчас покажем, положение меняется.

Прежде всего напомним, что, в силу теоремы 1 (§ 3), полярное отображение π, не являющееся нуль-системой, представимо симметрической α-формой $f(x, y)$, где $\alpha^2 = 1$ и $f(x, y) = f(y, x)^\alpha$ для любых x и y из A.

Предложение 2. *Пусть характеристика тела F отлична от 2, и пусть симметрическая полубилинейная форма $f(x, y)$ (над F-пространством A) представляет полярное отображение π. Тогда следующие свойства подпространств U и V F-пространства A эквивалентны:*

(I) $U \leqslant V^\pi$.

(II) $f(U, V) = 0$.

(III) $f(u, u) + f(v, v) = f(u + v, u + v)$ *для любых u из U и v из V.*

Если $f(x, x)$ интерпретировать как «квадрат длины вектора x», а равенство $f(U, V) = 0$ как «условие ортогональности подпространств U и V», то предложение 2 с полным правом можно назвать *теоремой Пифагора.*

Доказательство. Эквивалентность свойств (I) и (II) непосредственно следует из определения понятия «полярное отображение π представимо полубилинейной формой f». Прямым подсчетом можно проверить, что из свойства (II) следует свойство (III). Допустим теперь, что справедливо свойство (III), и предположим (вопреки утверждению), что существуют такие элементы u и v, содержащиеся соответственно в U и V, при которых $t = f(u, v) \neq 0$. Тогда элемент $t^{-1}u$ также содержится в U; поэтому,

[1]) То есть в геометрии, определяемой в векторном пространстве A полулинейной формой f. — *Прим. перев.*

в силу свойства (III),

$$f(t^{-1}u,\ t^{-1}u)+f(v,\ v)=f(t^{-1}u+v,\ t^{-1}u+v)=$$
$$=f(t^{-1}u,\ t^{-1}u)+f(t^{-1}u,\ v)+f(v,\ t^{-1}u)+f(v,v).$$

Отсюда, используя то, что f является симметрической α-формой, мы получаем

$$0=f(t^{-1}u,\ v)+f(v,\ t^{-1}u)=t^{-1}f(u,\ v)+f(v,\ u)t^{-\alpha}=$$
$$=1+f(u,\ v)^{\alpha}t^{-\alpha}=1+[t^{-1}f(u,\ v)]^{\alpha}=1+1;$$

но это противоречит нашему предположению, что характеристика тела F отлична от 2. Следовательно, $f(u,\ v)=0$, и этим показано, что из свойства (III) вытекает свойство (II).

Следствие 3. *Если характеристика тела F отлична от 2 и если симметрические полубилинейные формы f' и f'' представляют соответственно полярные отображения π' и π'', то $f'=f''$ тогда и только тогда, когда $f'(x,\ x)=f''(x,\ x)$ для каждого x из A.*

Доказательство. Пусть $f'(x,\ x)=f''(x,\ x)$ для каждого элемента x F-пространства A. В силу предложения 2, следующие утверждения относительно подпространств U и V F-пространства A эквивалентны:

$U\leqslant V^{\pi'}$; $f'(u,\ u)+f'(v,\ v)=f'(u+v,\ u+v)$ для любых u из U и v из V;

$f''(u,\ u)+f''(v,\ v)=f''(u+v,\ u+v)$ для любых u из U и v из V; $U\leqslant V^{\pi''}$.

Таким образом, из нашего предположения вытекает, что $U\leqslant V^{\pi'}$ тогда и только тогда, когда $U\leqslant V^{\pi''}$; но отсюда следует, что $\pi'=\pi''$. Поэтому, в силу предложения 3 (§ 1), в теле F существует такое число $c\neq 0$, что $f'(x,\ y)=f''(x,\ y)c$ для любых x и y из A. Так как нуль-системы представляются кососимметрическими билинейными формами (лемма 1, § 2), а симметрические полубилинейные формы не являются кососимметрическими формами, если характеристика основного тела отлична от 2, то в A найдется такой элемент w, что $f'(w,\ w)=f''(w,\ w)\neq 0$; поэтому $c=1$, т. е. $f'=f''$.

Следствие 4. *Пусть характеристика тела F отлична от 2, и пусть симметрическая полубилинейная форма f (над F-пространством A) представляет полярное отображение π. Тогда, если полулинейное преобразование σ удовлетворяет условию $f(x^{\sigma},\ x^{\sigma})=f(x,\ x)^{\sigma}$ для каждого x из A, то оно удовлетворяет условию $f(x^{\sigma},\ y^{\sigma})=f(x,\ y)^{\sigma}$ для любых x и y из A.*

Доказательство. Положим $g(x,\ y)=f(x^{\sigma},\ y^{\sigma})^{\sigma^{-1}}$. Нетрудно проверить, что g является симметрической полубилинейной формой и что g представляет некоторое полярное отображение

(а именно полярное отображение $\sigma^{-1}\pi\sigma$). Но так как $g(x, x) = f(x, x)$ для каждого x из A, то, в силу следствия 3, $f = g$, так что $f(x^\sigma, y^\sigma) = f(x, y)^\sigma$ для любых x и y из A.

Замечание 4. Для частного случая, когда σ является линейным преобразованием, следствие 4 утверждает, что σ сохраняет симметрическую полубилинейную форму f, если оно сохраняет «квадрат длины» $f(x, x)$.

Добавление IV

Полярные отображения, обладающие транзитивной группой

Пусть π — полярное отображение F-пространства A, ранг которого не меньше 3. Мы будем говорить, что группа полярного отображения π *транзитивна*, если для каждой пары точек P, Q F-пространства A существует такое π-допустимое проективное отображение, при котором точка P отображается на точку Q. Это, конечно, до некоторой степени ограниченное понятие транзитивности, поскольку в нем говорится лишь о точках, а не о произвольных подпространствах; в то же время оно несколько широкое, так как мы допускаем все π-допустимые проективные отображения. Оба эти замечания будут уточнены в процессе настоящего рассмотрения.

Если предположить, что группа полярного отображения π транзитивна, то справедливо одно из двух взаимно исключающих утверждений:

А. Каждая точка обладает свойством (N).

Б. Нет ни одной точки, обладающей свойством (N).

Это следует из того, что при π-допустимом проективном отображении точки, обладающие свойством (N), отображаются на точки, обладающие свойством (N). Действительно, если $P \leqslant P^\pi$ и $\sigma\pi = \pi\sigma$, где σ — проективное отображение, то $P^\sigma \leqslant P^{\pi\sigma} = P^{\sigma\pi}$.

Если каждая точка F-пространства A обладает свойством (N), то π будет нуль-системой. Если же ни одна из точек не обладает свойством (N), то из соотношения

$$U \cap U^\pi \leqslant U + U^\pi = (U \cap U^\pi)^\pi$$

следует, что в этом случае каждое подпространство будет неизотропным.

Теорема 1. *Если нуль-система π представима (кососимметрической билинейной) формой $f(x, y)$ и если P, Q — точки F-пространства A, то существует линейное преобразование σ, сохраняющее форму f и отображающее точку P на точку Q.*

Доказательство. Прежде всего отметим, что, в силу леммы 1 (§ 2), нуль-системы представимы кососимметрическими билинейными формами и что, следовательно, F является полем.

Рассмотрим теперь произвольную точку X. Так как X^π является гиперплоскостью, то существует точка Y, не принадлежащая X^π; так как $X \leqslant X^\pi$, то точка Y не совпадает с точкой X. Легко проверить, что прямая $L = X + Y$ неизотропна. Пусть $X = Fx$ и $Y = Fy$. Тогда $f(x, y) = -f(y, x) \neq 0$; элементы x и y всегда можно подобрать так, что $f(x, y) = 1$ [если $f(x, y)$ не равно 1, то x нужно заменить элементом $f(x, y)^{-1}x$]; предположим, что это уже сделано.

Так как прямая L неизотропна, то также неизотропно подпространство L^π и, в силу следствия 2 (§ 1), $A = L + L^\pi$. Из предложения 1 (§ 2) вытекает существование в подпространстве L^π такого базиса x_i', x_i'', $i = 1, \ldots, k$, что

$$f(x_i', x_i'') = -f(x_i'', x_i') = 1 \text{ для } i = 1, \ldots, k;$$

$$f(x_i', x_j') = f(x_i', x_j'') = f(x_j'', x_i') = f(x_j'', x_i'') = 0 \text{ для } i \neq j.$$

Применяя только что проведенное рассуждение к точкам P и Q, мы найдем в F-пространстве A такие базисы p, p_0, p_i', p_i'' и q, q_0, q_i', q_i'', что

$$1 = f(p, p_0) = -f(p_0, p) = f(p_i', p_i'') = -f(p_i'', p_i') = \\ = f(q, q_0) = -f(q_0, q) = f(q_i', q_i'') = -f(q_i'', q_i')$$

и $f(x, y) = 0$ для любой пары элементов x и y одного из этих базисов, отличной от перечисленных выше.

Существует, и притом только одно, такое линейное преобразование σ, при котором $p^\sigma = q$, $p_0^\sigma = q_0$, $p_i'^\sigma = q_i'$, $p_i''^\sigma = q_i''$ для $i = 1, \ldots, k$. Легко проверить, что σ сохраняет форму f; этим теорема 1 полностью доказана.

Замечание 1. Слегка изменяя метод, которым была доказана предыдущая теорема, можно доказать следующее утверждение:

Если U и V — неизотропные подпространства одинакового ранга, то существует линейное преобразование σ, сохраняющее форму f и отображающее U на V[1]).

Замечание 2. Совершенно ясно, как найти неизотропную прямую L' и строго изотропную прямую L'' (относительно нуль-системы); легко проверить, что не существует такого π-допустимого проективного отображения, при котором L' отображается на L''. Таким образом, группа нуль-системы транзитивна относительно точек и не транзитивна относительно прямых.

[1]) Здесь, так же как и в теореме 1, предполагается, что полярное отображение, представимое билинейной формой f, является нуль-системой. — *Прим. перев.*

Группа линейных преобразований, сохраняющих данную кососимметрическую билинейную форму $f(x, y)$, в настоящее время называется *симплектической*; из теоремы 1 следует, что симплектическая группа транзитивна относительно точек и, как было показано в замечании 1, относительно неизотропных подпространств ранга $2i$.

Случай Б, в котором все подпространства являются неизотропными, оказывается более сложным по сравнению с тем, когда полярное отображение является нуль-системой.

Теорема 2. *Если α-форма $f(x, y)$ представляет полярное отображение π и если $f(w, w) = 1$ для некоторого элемента w F-пространства A, то следующие свойства эквивалентны:*

(I) *Для произвольной пары точек P и Q F-пространства A существует линейное преобразование, сохраняющее форму f и отображающее P на Q.*

(II) *Для каждого элемента $x \neq 0$ из A в теле F существует такое число $y \neq 0$, что $f(x, x) = yy^{\alpha}$.*

(III) *F, α и f обладают следующими двумя свойствами:*

(а) *Для каждого числа s из F в теле F существует такое число $t \neq 0$, что $1 + ss^{\alpha} = tt^{\alpha}$.*

(б) *В F-пространстве A существует такой базис $b_1, \ldots, b_n$, что*

$$f(b_i, b_j) = \begin{cases} 1 \text{ для } i = j, \\ 0 \text{ для } i \neq j. \end{cases}$$

Доказательство. Предположим сначала, что выполняется свойство (I). Если $x \neq 0$, то Fx является точкой; поэтому, в силу свойства (I), существует линейное преобразование σ, сохраняющее форму f и отображающее точку Fw на точку Fx. Следовательно, в F существует такое число $v \neq 0$, что $w^{\sigma} = vx$. Но σ сохраняет форму f; поэтому

$$1 = f(w, w) = f(w^{\sigma}, w^{\sigma}) = f(vx, vx) = vf(x, x)v^{\alpha},$$

откуда $f(x, x) = yy^{\alpha}$, где $y = v^{-1}$. Таким образом, свойство (II) следует из свойства (I).

Пусть теперь справедливо свойство (II). Тогда, если Fx — точка, то в F существует такое число $y \neq 0$, что $f(x, x) = yy^{\alpha}$. Положим $x' = y^{-1}x$. Тогда $Fx = Fx'$ и $f(x', x') = y^{-1}f(x, x)y^{-\alpha} = 1$; тем самым мы показали, что каждую точку Z можно представить в виде $Z = Fz$, причем $f(z, z) = 1$.

Если P — некоторая точка, то, как было показано в предыдущем абзаце, $f(P, P) \neq 0$. Следовательно, P не является N-точкой, и поэтому P можно вложить в некоторое максимальное 0-множество точек $P = P_1, \ldots, P_n$. Поскольку в A нет ни одной N-точки, из утверждений (а), (б) леммы 4 (§ 4) вытекает, что точки P_i образуют базис F-пространства A. В силу результата предыду-

щего абзаца, существуют такие элементы p_i, что $P_i = Fp_i$ и $f(p_i, p_i) = 1$. Так как точки P_i образуют 0-множество, то $P_i \leqslant P_j^\perp$ для $i \neq j$ и, следовательно, $f(p_i, p_j) = 0$ для $i \neq j$. Очевидно, наконец, что элементы p_i образуют базис F-пространства A; таким образом, показано, что из свойства (II) следует свойство (III.б).

Если Q — другая точка, то подобным же образом можно найти в F-пространстве A такой базис $q_1, \ldots, q_n$, что $Q = Fq_1$ и

$$f(q_i, q_j) = \begin{cases} 1 \text{ для } i = j, \\ 0 \text{ для } i \neq j. \end{cases}$$

Существует, и притом только одно, такое линейное преобразование σ F-пространства A, при котором $p_i^\sigma = q_i$ для $i = 1, \ldots, n$. Простым подсчетом можно проверить, что σ сохраняет форму f; очевидно также, что $P^\sigma = Q$. Таким образом, из свойства (II) следует свойство (I).

Пусть опять справедливо свойство (II). Тогда, как уже было показано, в F-пространстве A существует такой базис $b_1, \ldots, b_n$, что

$$f(b_i, b_j) = \begin{cases} 1 \text{ для } i = j, \\ 0 \text{ для } i \neq j. \end{cases}$$

Если теперь s — произвольное число из F, то $b_1 + sb_2 \neq 0$; отсюда и из свойства (II) следует существование такого числа $t \neq 0$, что

$$tt^\alpha = f(b_1 + sb_2, b_1 + sb_2) = 1 + ss^\alpha.$$

Таким образом, свойство (III.а) также следует из свойства (II).

Пусть, наконец, справедливо свойство (III). Тогда мы прежде всего докажем следующее утверждение.

(П) *Если* $x_1, \ldots, x_k$ — *отличные от* 0 *числа из тела* F, *то в* F *существует такое число* $y \neq 0$, *что* $\sum_{i=1}^{k} x_i x_i^\alpha = yy^\alpha$.

Это утверждение справедливо, очевидно, если $k = 1$; поэтому мы сделаем индуктивное предположение, что утверждение (П) справедливо для сумм с меньшим чем k числом слагаемых (где $k > 1$). Тогда существует такой элемент $z \neq 0$, что $\sum_{i=1}^{k-1} x_i x_i^\alpha = zz^\alpha$. Из свойства (III.а) вытекает существование в теле F элемента $t \neq 0$, удовлетворяющего условию

$$1 + (z^{-1}x_k)(z^{-1}x_k)^\alpha = tt^\alpha.$$

Поэтому

$$\sum_{i=1}^{k} x_i x_i^\alpha = zz^\alpha + x_k x_k^\alpha = z[1 + (z^{-1}x_k)(z^{-1}x_k)^\alpha]z^\alpha = ztt^\alpha z^\alpha = yy^\alpha,$$

где $y = zt \neq 0$, чем и завершается индуктивное доказательство утверждения (П).

Если теперь $x \neq 0$ — элемент из A, то $x = \sum_{i=1}^{n} x_i b_i$, где x_i — числа из F, по крайней мере одно из которых отлично от 0, а элементы b_i образуют базис F-пространства A, нормализованный согласно условию (III.б). Поэтому $f(x, x) = \sum_{i=1}^{n} x_i x_i^{\alpha}$, и так как не все числа x_i равны 0, то, в силу утверждения (П), существует такое число $y \neq 0$, что $\sum_{i=1}^{n} x_i x_i^{\alpha} = yy^{\alpha}$; этим доказано, что свойство (II) следует из свойства (III). Тем самым теорема 2 полностью доказана.

Замечание 3. Отметим, что свойство (П) инволюторного инверсного автоморфизма тела F следует исключительно из свойства (III.а). Пары (F, α), для которых справедливы (эквивалентные) свойства (П) и (III.а), мы будем называть *α-пифагоровыми*. Из этих свойств следует, очевидно, что характеристика тела F равна 0. Заметим, кроме того, что, по свойству (е) добавления I, в теле F, обладающем областью α-положительности, $\sum_{i=1}^{n} x_i x_i^{\alpha} \neq 0$, если не все x_i равны 0. Известно, что это последнее свойство (которое, как было показано, выполняется, если F, α есть пифагорова пара) эквивалентно существованию области α-положительности, по крайней мере в случае, когда $\alpha = 1$ (см. теорию действительных полей Артина — Шрейера, например, в книге Ван-дер-Вардена [2]).

Замечание 4. Если для α-формы f в F-пространстве A существует базис b_i, нормализованный согласно условию (III.б), то

$$f(x, y) = \sum_{i=1}^{n} x_i y_i^{\alpha},$$

так что такая форма f определяется при данном α по существу однозначно.

Следствие 1. *Пусть α-форма $f(x, y)$ представляет полярное отображение π, $f(w, w) = 1$ для некоторого элемента w F-пространства A и совокупность F, α, f обладает свойствами* (I) — (III) *из теоремы 2. Тогда*:

(а) *Если $0 < U_1 < \ldots < U_{n-1} < A$ и $0 < V_1 < \ldots < V_{n-1} < A$ — две цепочки подпространств и если $n = r(A)$, то существует линейное преобразование σ, сохраняющее форму f и удовлетворяющее условиям $U_i^{\sigma} = V_i$ для $i = 1, \ldots, n$.*

(б) *Если U и V — подпространства одного и того же ранга, то существует линейное преобразование, сохраняющее форму f и отображающее U на V.*

Доказательство. Пусть нам даны такие подпространства U_i, что

$$0 = U_0 < U_1 < \ldots < U_{n-1} < U_n = A.$$

Тогда из $r(A) = n$ следует $r(U_i) = i$. Если хотя бы одно из подпространств U_i было изотропно, то в A существовали бы N-точки; поэтому U_i — неизотропные подпространства. Следовательно, $A = U_i + U_i^{\pi}$; отсюда вытекает, что $U_{i+1} = U_i + [U_{i+1} \cap U_i^{\pi}]$. При доказательстве теоремы 2 было установлено, что точку $U_{i+1} \cap U_i^{\pi}$ можно представить в виде Fu_{i+1}, причем $f(u_{i+1}, u_{i+1}) = 1$ (для $0 \leqslant i < n$). Элементы $u_1, \ldots, u_n$ образуют базис F-пространства A, удовлетворяющий следующим условиям:

$$U_i = \sum_{j=1}^{i} Fu_j, \qquad f(u_i, u_j) = \begin{cases} 1 & \text{для } i = j, \\ 0 & \text{для } i \neq j. \end{cases}$$

Подобным же образом с цепочкой подпространств V_i мы свяжем базис $v_1, \ldots, v_n$ F-пространства A, удовлетворяющий аналогичным условиям. Существует, и притом только одно, такое линейное преобразование σ F-пространства A, при котором $u_i^{\sigma} = v_i$ для $i = 1, \ldots, n$. Очевидно, что $U_i^{\sigma} = V_i$ и что σ сохраняет форму f. Тем самым утверждение (а) доказано; утверждение (б) легко следует из (а), поскольку подпространства U и V можно представить как i-е члены $[i = r(U) = r(V)]$ цепочек такого вида, какие рассматриваются в утверждении (а).

Замечание 5. Сравним следствие 1 (б) с замечанием 2. Мы видим, что условия (I) — (III) теоремы 2 являются необходимыми и достаточными для «полной транзитивности».

Замечание 6. Если $\alpha = 1$, то группа $\Gamma(\pi)$ называется *ортогональной*; эта группа называется *унитарной*, если F — поле и $\alpha \neq 1$; при этом, конечно, дополнительно предполагается, что полярное отображение π обладает свойствами транзитивности теоремы 2 и следствия 1. В случае, когда тело F некоммутативно, для соответствующих групп пока еще нет общепринятых названий. Читатель должен обратить внимание на то, что из существования полярного отображения π, обладающего свойствами транзитивности теоремы 2 и следствия 1, не вытекает коммутативность основного тела F. Например, если F — тело действительных кватернионов и α — инволюторный инверсный автоморфизм тела F, отображающий каждый кватернион в сопряженный ему кватернион, то, используя замечание 4, можно построить полярное отображение, обладающее указанными свойствами транзитивности [см. теорему 2, (III)].

§ 6. Подпространства, неизотропные относительно полярного отображения

Полярное отображение не определяется, конечно, подпространствами, относительно него строго изотропными, поскольку легко построить линейные многообразия, обладающие большим числом различных полярных отображений, относительно которых 0 будет единственным строго изотропным подпространством. С другой стороны, полярное отображение полностью определяется инволюторной перестановкой, индуцированной этим полярным отображением на множестве подпространств, относительно него неизотропных. Убедиться в справедливости этого утверждения легко на основании леммы (1.а), выведенной при доказательстве теоремы 1 (§ 5); этот же результат мы получим в качестве следствия рассмотрений, проводимых в настоящем параграфе. При этом следует заметить, что одна система неизотропных подпространств (без индуцированного в ней инволюторного преобразования) не определяет полярное отображение, ибо, как было замечено выше, различные полярные отображения одного и того же линейного многообразия могут обладать тем свойством, что каждое подпространство является относительно них неизотропным.

Мы поставим нашу задачу следующим образом. Пусть (F, A) будет линейным многообразием, ранг которого не меньше 3; рассмотрим произвольное множество Θ подпространств F-пространства A и инволюторную перестановку τ, определенную в множестве Θ. Задача состоит в том, чтобы найти необходимые и достаточные условия, при которых существует такое полярное отображение σ F-пространства A, что Θ будет совокупностью всех подпространств, неизотропных относительно σ, и τ совпадает с перестановкой подпространств, содержащихся в Θ, индуцированной полярным отображением σ. Наши основные результаты, относящиеся к этой задаче, можно сформулировать следующим образом. (Вместо выражения «подпространство, принадлежащее Θ», мы будем употреблять выражение «Θ-пространство».)

Теорема единственности. *Существует не более одного полярного отображения, для которого Θ является совокупностью всех неизотропных подпространств и которое индуцирует в Θ перестановку, совпадающую с τ.*

Теорема существования. *Тогда и только тогда существует такое полярное отображение F-пространства A, для которого Θ будет совокупностью всех неизотропных подпространств и которое индуцирует в Θ данную инволюторную перестановку τ, когда пара Θ, τ удовлетворяет следующим условиям:*

I. *Θ содержит 0 и A.*

II. *$A = S + S^{\tau}$ для каждого S из Θ.*

III. *Θ-пространства V_i и W_i тогда и только тогда удовле-*

творяют условию $V_1 \cap \ldots \cap V_m \leqslant W_1 + \ldots + W_n$, когда

$$W_1^\tau \cap \ldots \cap W_n^\tau \leqslant V_1^\tau + \ldots + V_m^\tau.$$

IV. *Если M' и M'' являются максимальными Θ-пространствами, содержащимися в подпространстве S, то $S \cap M'^\tau = S \cap M''^\tau$.*

Если N' и N'' являются минимальными Θ-пространствами, содержащими подпространство S, то $S + N'^\tau = S + N''^\tau$.

V. *Если подпространство S F-пространства A содержится в некотором Θ-пространстве, отличном от A, то S совпадает с пересечением всех Θ-пространств, содержащих S.*

Если подпространство S F-пространства A содержит некоторое Θ-пространство, отличное от 0, то S совпадает с суммой всех Θ-пространств, содержащихся в S.

VI. *Если T — такое подпространство F-пространства A, что 0 является единственным Θ-пространством, содержащимся в T, и A — единственным Θ-пространством, содержащим T, то*

(а) $r(A) = 2r(T)$;

(б) $M \leqslant T + N$ *тогда и только тогда, когда* $T \cap N^\tau \leqslant M^\tau$ *для любых* M, N *из* Θ.

Чтобы доказать необходимость условий I — VI и теорему единственности, мы рассмотрим сначала полярное отображение σ линейного многообразия (F, A), ранг которого $r(A)$ не меньше 3. Обозначим через $\Theta(\sigma)$ совокупность всех неизотропных относительно σ подпространств F-пространства A. В силу следствия 2 (§ 1), подпространство U тогда и только тогда принадлежит $\Theta(\sigma)$, когда выполняется одно из следующих эквивалентных между собой условий:

$$U \cap U^\sigma = 0, \quad A = U \dotplus U^\sigma, \quad A = U + U^\sigma.$$

Это показывает, что множество $\Theta(\sigma)$ удовлетворяет условиям I и II; отсюда же вытекает, что U тогда и только тогда принадлежит $\Theta(\sigma)$, когда к $\Theta(\sigma)$ принадлежит U^σ. Следовательно, полярное отображение σ индуцирует в множестве $\Theta(\sigma)$ инволюторную перестановку; эту перестановку мы также будем обозначать через σ. Справедливость условия III непосредственно следует из того, что полярное отображение переводит сумму подпространств в пересечение образов этих подпространств и, обратно, пересечение подпространств в сумму их образов. Для того, чтобы доказать справедливость в $\Theta(\sigma)$ свойств IV — VI, мы предварительно докажем несколько лемм, которые интересны и сами по себе.

Лемма 1. *Если U и V — такие подпространства F-пространства A, что*

$$0 = U \cap U^\sigma \cap V, \qquad A = U + U^\sigma + V,$$
$$U = (U \cap U^\sigma) + V, \qquad U = (U + U^\sigma) \cap V,$$

то V является максимальным неизотропным подпространством, содержащимся в U[1]).

то V является минимальным неизотропным подпространством, содержащим U.

Доказательство. Прежде всего заметим, что если справедливо одно из этих утверждений, то справедливо и второе, поскольку они двойственны друг другу; таким образом, нам достаточно доказать только одно из них, например левое.

Пусть U и V — такие подпространства, что $U=(U\cap U^\sigma)\dotplus V$. Тогда, используя закон Дедекинда, мы последовательно получаем (принимая во внимание соотношения $V\leqslant U$ и $U^\sigma\leqslant V^\sigma$), что

$$U^\sigma=[(U\cap U^\sigma)+V]^\sigma=(U^\sigma+U)\cap V^\sigma=U^\sigma+(U\cap V^\sigma),$$

откуда $U\cap V^\sigma\leqslant U^\sigma$,

$$V\cap V^\sigma=V\cap U\cap V^\sigma=V\cap U\cap V^\sigma\cap U^\sigma=0.$$

Тем самым показана неизотропность подпространства V. Если теперь W — такое неизотропное подпространство, содержащееся в U, что $V\leqslant W$, то

$$W=V\dotplus(W\cap U\cap U^\sigma)=V\dotplus(W\cap U^\sigma)=V,$$

поскольку $V\leqslant W\leqslant U=V\dotplus(U\cap U^\sigma)$ и, следовательно,

$$W\cap U^\sigma\leqslant W\cap W^\sigma=0.$$

Таким образом, лемма полностью доказана.

Проверка условия IV. Так как оба требования, сформулированные в условии IV, двойственны друг другу, то достаточно доказать справедливость одного из них, например левого. Таким образом, пусть S есть подпространство F-пространства A и M', M'' — максимальные неизотропные подпространства, содержащиеся в S. Тогда из $M'\leqslant S$ и $A=M'\dotplus M'^\sigma$ мы выведем, что $S=M'\dotplus(S\cap M'^\sigma)$; далее, так как $S^\sigma\leqslant M''^\sigma$, то

$$S\cap S^\sigma\leqslant S\cap M''^\sigma.$$

Из полученного включения, в силу принципа дополнения (гл. II, § 1), вытекает существование такого подпространства H, что

$$S\cap M''^\sigma=(S\cap S^\sigma)\dotplus H.$$

Таким образом,

$$S=(S\cap S^\sigma)\dotplus H\dotplus M';$$

[1]) Это утверждение доказывалось ранее в лемме 2 (§ 4). — *Прим. перев.*

отсюда и из леммы 1 вытекает, что $H \dotplus M'$ является неизотропным подпространством. Но M' — максимальное неизотропное подпространство, содержащееся в S; следовательно, $H \dotplus M' = M'$, т. е. $H = 0$ и $S \cap M'^{\sigma} = S \cap S^{\sigma}$. Подобным же образом показывается, что

$$S \cap M''^{\sigma} = S \cap S^{\sigma},$$

чем и завершается проверка выполнения в $\Theta(\sigma)$ условия IV. Заметим, что мы попутно убедились в справедливости следующего утверждения.

Следствие 1. *Пусть U и V — подпространства F-пространства A.*

Если V — максимальное неизотропное подпространство, содержащееся в U, то

$$U \cap V^{\sigma} = U \cap U^{\sigma}.$$

Если V — минимальное неизотропное подпространство, содержащее U, то

$$U + V^{\sigma} = U + U^{\sigma}.$$

Проверка условия V. Здесь также достаточно проверить только одно из двойственных друг другу утверждений: мы докажем справедливость правого утверждения. Пусть подпространство S содержит некоторое неизотропное подпространство, отличное от 0. Тогда S содержит максимальное неизотропное подпространство M, которое тем более отлично от 0. В силу следствия 1, $S \cap S^{\sigma} = S \cap M^{\sigma}$; поэтому из $M \leqslant S$ и $A = M \dotplus M^{\sigma}$ вытекает, что $S = M \dotplus (S \cap M^{\sigma}) = M \dotplus (S \cap S^{\sigma})$. Поскольку $M \neq 0$, мы имеем $M = Fm \dotplus N$, где m — отличный от 0 элемент F-пространства A. Если t — элемент, принадлежащий $S \cap S^{\sigma}$, то

$$S = M \dotplus (S \cap S^{\sigma}) = Fm \dotplus N \dotplus (S \cap S^{\sigma}) = F(m+t) \dotplus N \dotplus (S \cap S^{\sigma});$$

отсюда, по лемме 1, мы получаем, что подпространство $F(m+t) \dotplus N$ неизотропно. Таким образом, оба элемента m и $m+t$ принадлежат неизотропным подпространствам, содержащимся в S, и, следовательно, элемент t принадлежит сумме всех неизотропных подпространств, содержащихся в S. Тем самым показано, что $S \cap S^{\sigma}$ является частью суммы всех неизотропных подпространств, содержащихся в S; отсюда ясно, что S совпадает с суммой всех неизотропных подпространств, в нем содержащихся.

Лемма 2. *Подпространство S тогда и только тогда удовлетворяет условию $S = S^{\sigma}$, когда 0 является единственным неизотропным подпространством, содержащимся в S, и A — единственным неизотропным подпространством, содержащим S.*

Доказательство. Пусть $S = S^{\sigma}$, и пусть U — неизотропное подпространство, содержащееся в S. Тогда $U \leqslant S = S^{\sigma} \leqslant U^{\sigma}$ и, следовательно, $U = U \cap U^{\sigma} = 0$; подобным же образом доказывается,

что A является единственным неизотропным подпространством, содержащим S.

Обратно, пусть 0 — единственное неизотропное подпространство, содержащееся в S, и A — единственное неизотропное подпространство, содержащее S. В S содержится такое подпространство T, что $S = T \dotplus (S \cap S^\sigma)$. По лемме 1, T есть неизотропное подпространство; следовательно, в силу наших предположений, $T = 0$, а тем самым $S = S \cap S^\sigma$, т. е. $S \leqslant S^\sigma$. Подобным же образом (или из двойственных соображений) получим, что $S^\sigma \leqslant S$. Таким образом, $S = S^\sigma$, что и требовалось доказать.

Проверка условия VI. Пусть T — такое подпространство F-пространства A, что 0 является единственным неизотропным подпространством, содержащимся в T, и A — единственным неизотропным подпространством, содержащим T. Тогда, по лемме 2, $T = T^\sigma$; отсюда и из следствия 1 (§ 1) вытекает, что $r(A) = r(T) + r(T^\sigma) = 2r(T)$. Предположим теперь, что для неизотропных подпространств M и N имеет место соотношение $M \leqslant T + N$. Тогда, используя основные свойства полярных отображений, мы получим, что

$$T \cap N^\sigma = T^\sigma \cap N^\sigma = (T + N)^\sigma \leqslant M^\sigma;$$

обратное утверждение следует из двойственных соображений.

Таким образом, необходимость условий, сформулированных в теореме существования, полностью доказана. Доказательство теоремы единственности непосредственно следует теперь из свойства V и леммы 2; детали доказательства мы оставляем читателю.

Пусть теперь множество Θ подпространств F-пространства A и инволюторная перестановка τ, определенная в Θ, удовлетворяют условиям I — VI. Если S — произвольное подпространство F-пространства A, то обозначим через

S_Θ совокупность всех Θ-пространств, содержащихся в S, и через S^0 — пересечение всех X^τ для X из S_Θ.

S^Θ совокупность всех Θ-пространств, содержащих S, и через S_0 — сумму всех X^τ для X из S^Θ.

При помощи этих двух операций мы построим требуемое полярное отображение. Наши рассмотрения значительно упростятся после следующих замечаний. Из условия III в частном случае $m = n = 1$ следует, что для Θ-пространств S и T включение $S < T$ справедливо тогда и только тогда, когда $T^\tau < S^\tau$. Таким образом, инволюторная перестановка τ множества Θ является «неполным полярным отображением». Кроме того, все условия I — VI двойственны себе; поэтому одновременно с каждым предложением,

вытекающим из этих условий, справедливо и двойственное предложение. Для X из S_Θ и Y из S^Θ мы имеем $X \leqslant S \leqslant Y$. Поэтому $Y^\tau \leqslant X^\tau$; отсюда легко следует, что

$$S_0 \leqslant S^0.$$

Теперь мы выведем несколько свойств указанных выше операций.

(1) Если S^Θ не состоит лишь из одного A, то $S_{0\Theta} = S^{\Theta\tau}$; аналогично, если S_Θ не состоит лишь из одного 0, то $S^{0\Theta} = S_\Theta^\tau$.

Доказательство. Если X содержится в S^Θ, то $S \leqslant X$; из определения же подпространства S_0 следует, что $X^\tau \leqslant S_\Theta$ и поэтому X^τ принадлежит множеству $S_{0\Theta}$. Таким образом, $S^{\Theta\tau} \leqslant S_{0\Theta}$. Так как S^Θ содержит Θ-пространство, отличное от A, то, по условию V, подпространство S совпадает с пересечением всех Θ-пространств, содержащихся в S^Θ. Из конечности ранга F-пространства A вытекает существование в S^Θ конечного множества Θ-пространств, пересечение которых совпадает с S; из тех же соображений видно, что в $S^{\Theta\tau}$ существует конечное множество Θ-пространств, сумма которых равна S_0. Следовательно, можно выбрать такое конечное множество Θ-пространств $X_1, \ldots, X_k$, что одновременно

$$S = X_1 \cap \ldots \cap X_k \quad \text{и} \quad S_0 = X_1^\tau + \ldots + X_k^\tau.$$

Отсюда, из условия III и из инволюторности перестановки τ мы получаем, что Θ-пространство X тогда и только тогда принадлежит множеству $S_{0\Theta}$, когда $S \leqslant X^\tau$; но последнее включение эквивалентно тому, что X^τ содержится в S^Θ. Теперь требуемое равенство $S_{0\Theta} = S^{\Theta\tau}$ непосредственно следует из инволюторности перестановки τ. Этим доказано первое утверждение предложения (1); второе утверждение двойственно ему.

(2) Если S_Θ не состоит лишь из одного 0 и S^Θ не состоит лишь из одного A, то $S_0 = S^0$.

Доказательство. Из наших предположений следует, что S одновременно является суммой всех Θ-пространств, принадлежащих S_Θ, и пересечением всех Θ-пространств, принадлежащих S^Θ. Поэтому, используя конечность ранга F-пространства A, мы, как и при доказательстве предыдущего утверждения, сможем выбрать такие Θ-пространства $X_1, \ldots, X_h$ и $Y_1, \ldots, Y_k$, что одновременно

$$S = X_1 + \ldots + X_h = Y_1 \cap \ldots \cap Y_k,$$

$$S^0 = X_1^\tau \cap \ldots \cap X_h^\tau, \; S_0 = Y_1^\tau + \ldots + Y_k^\tau.$$

Но из равенства $Y_1 \cap \ldots \cap Y_k = X_1 + \ldots + X_h$, в силу условия III, вытекает, что

$$X_1^\tau \cap \ldots \cap X_h^\tau \quad Y_1 + \ldots + Y_k^\tau,$$

т. е. $S^0 \leqslant S_0$. С другой стороны, как было показано выше, обратное включение $S_0 \leqslant S^0$ справедливо всегда. Следовательно, $S_0 = S^0$ [1]).

Теперь сделаны все необходимые приготовления для того, чтобы *следующим образом определить операцию* σ *для всех подпространств* S *F-пространства* A:

(а) Если S_Θ содержит Θ-пространство, отличное от 0, то $S^\sigma = S^0$.

(б) Если S_Θ содержит только 0 и S^Θ содержит только A, то $S^\sigma = S$.

(в) Если S^Θ содержит Θ-пространство, отличное от A, то $S^\sigma = S_0$.

Так определенная операция σ отображает каждое подпространство S F-пространства A на одно и только одно подпространство S^σ того же пространства, поскольку, как следует из утверждения (2), если к S применимы оба правила (а) и (в), то они дают один и тот же результат.

Пусть, в частности, S будет Θ-пространством. Если $S = 0$, $S^\tau = A$, то $S_0 = A$; поэтому, пользуясь правилом (в), мы получаем, что $0^\sigma = A$; подобным же образом убеждаемся, что $A^\sigma = 0$. Если же Θ-пространство S отлично от 0 и A, то S одновременно принадлежит и S^Θ и S_Θ; поэтому $S_0 = S^0 = S^\tau$, так что и в этом случае $S^\sigma = S^\tau$. Докажем теперь, что

(3) $\sigma^2 = 1$.

Для того, чтобы доказать это утверждение, проверим, что $S^{\sigma^2} = S$ для каждого подпространства S F-пространства A. Это равенство справедливо, очевидно, если S является Θ-пространством, ибо в этом случае σ совпадает с инволюторной перестановкой τ; также тривиален случай, когда 0 – единственное Θ-пространство, содержащееся в S_Θ, и A – единственное Θ-пространство, содержащее S^Θ [правило (б)]. Если множество S_Θ содержит Θ-пространство, отличное от 0, то $S^\sigma = S^0$ и $S^{0\Theta} = S^\tau_\Theta$. Но тогда $S^{\sigma^2} = (S^0)_0$ совпадает с суммой всех Θ-пространств, принадлежащих $S^{0\Theta\tau} = S_\Theta$; последнее равенство имеет место ввиду инволюторности перестановки τ. Отсюда и из условия V вытекает, что $S^{\sigma^2} = S$. Пользуясь соображениями двойственности, мы получим такой же результат в случае, когда S^Θ содержит Θ-пространство, отличное от A; тем самым утверждение (3) полностью доказано.

Из утверждения (3), в частности, следует, что σ является инволюторной перестановкой в системе всех подпространств F-пространства A, совпадающей на Θ с перестановкой τ.

---

[1]) Окончание доказательства свойства (2) несколько изменено, так как в оригинале в этом месте содержится неточность.—*Прим. перев.*

(4) σ *является полярным отображением F-пространства A.*

Для доказательства этого утверждения нам нужно только показать, что из $S \leqslant T$ следует $T^\sigma \leqslant S^\sigma$. Чтобы сделать это, рассмотрим следующие возможные случаи.

Случай 1: Множество S_Θ содержит Θ-пространство, отличное от 0. В этом случае из $S \leqslant T$ следует, что S_Θ является частью множества T_Θ и поэтому T_Θ содержит Θ-пространство, отличное от 0. Следовательно, $T^\sigma = T^\Theta \leqslant S^\Theta = S^\sigma$.

Случай 2: T^Θ содержит Θ-пространство, отличное от A. Из соображений, двойственных к тем, какие были использованы при рассмотрении случая 1, мы убедимся в справедливости требуемого включения $T^\sigma \leqslant S^\sigma$.

Случай 3: S_Θ состоит лишь из одного 0, а T^Θ состоит лишь из одного A.

Здесь мы разберем несколько подслучаев.

Случай 3.1: S^Θ содержит Θ-пространство, отличное от A, а T_Θ содержит Θ-пространство, отличное от 0. В этом случае существует конечное множество таких Θ-пространств X_i, Y_j, что одновременно

$$S = X_1 \cap \ldots \cap X_h,\ S^\sigma = X_1^\tau + \ldots + X_h^\tau,$$

$$T = Y_1 + \ldots + Y_k,\ T^\sigma = Y_1^\tau \cap \ldots \cap Y_k^\tau;$$

из этих равенств, включения $S \leqslant T$ и условия III вытекает, что $T^\sigma \leqslant S^\sigma$.

Случай 3.2: S^Θ состоит лишь из одного A, а T_Θ содержит Θ-пространство, отличное от 0. Здесь, в силу (б), $S^\sigma = S$, а по правилу (а), $T^\sigma = T^0$. Сейчас нам понадобится следующий вспомогательный результат.

(+) Если M — отличное от 0 Θ-пространство, то

$$(S+M)^\sigma = S \cap M^\sigma = S \cap M^\tau.$$

Очевидно, что $M \neq 0$ содержится в $(S+M)_\Theta$; поэтому $(S+M)^\sigma = (S+M)^0$. Но из условия VI (б) вытекает, что Θ-пространство X тогда и только тогда принадлежит $(S+M)_\Theta$, когда $S \cap M^\tau \leqslant X^\tau$. Таким образом, $(S+M)^\sigma$ совпадает с пересечением всех Θ-пространств, принадлежащих $(S \cap M^\tau)^\Theta$. В силу же условия V, это пересечение равно $S \cap M^\tau$; отсюда следует, что $(S+M)^\sigma = S \cap M^\tau = S \cap M^\sigma$.

Так как T^σ есть пересечение всех X^τ для $X \neq 0$ из T_Θ, то из утверждения (+) следует, что $S \cap T^\sigma$ совпадает с пересечением всех $S \cap X^\tau = (S+X)^\sigma$ для $X \neq 0$ из T_Θ. Но $(S+X)^\sigma$ совпадает с пересечением всех Θ-пространств Y^τ, где Y содержится

в $(S+X)_\Theta$, ибо в этом множестве содержится Θ-пространство $X \neq 0$. Таким образом, $S \cap T^\sigma$ совпадает с пересечением всех Θ-пространств Z, удовлетворяющих условию:

Существует такое Θ-пространство X, что $X \leqslant T$ и

$$Z^\tau \leqslant S+X.$$

Так как $S \leqslant T$, то указанное условие эквивалентно тому, что $Z^\tau \leqslant T$, ибо в качестве X мы можем выбрать Z^τ; отсюда следует, что $S \cap T^\sigma$ совпадает с пересечением всех Θ-пространств X^τ, где X содержится в T_Θ. Таким образом, $S \cap T^\sigma = T^\sigma$, откуда $T^\sigma < S = S^\sigma$, что и требовалось доказать.

Случай 3.3: S^Θ содержит Θ-пространство, отличное от A, а T_Θ состоит лишь из одного 0. В этом случае справедливость включения $T^\sigma \leqslant S^\sigma$ доказывается с помощью рассуждений, двойственных к тем, какими мы пользовались при рассмотрении случая 3.2.

Случай 3.4: S^Θ состоит лишь из одного A, и T_Θ состоит лишь из одного 0. В этом случае, в силу правила (б), $T = T^\sigma$ и $S = S^\sigma$; отсюда и из условия VI (а) вытекает, что $r(S) = r(A)/2 = r(T)$. Поэтому, используя конечность ранга F-пространства A и включение $S \leqslant T$, мы получаем, что $T^\sigma = T = S = S^\sigma$.

Таким образом, мы проверили справедливость нужного нам включения во всех возможных случаях и тем самым полностью доказали утверждение о том, что σ является полярным отображением.

(5) *Подпространство S тогда и только тогда неизотропно относительно полярного отображения σ, когда оно принадлежит Θ.*

Так как полярное отображение σ на множестве Θ совпадает с перестановкой τ, то, по условию II, все Θ-пространства неизотропны. Обратно, пусть S — неизотропное относительно σ подпространство. Тогда, ввиду правила (б), невозможно, чтобы 0 было единственным Θ-пространством, содержащимся в S, и в то же время A было единственным Θ-пространством, содержащим S. Ввиду двойственности (в частности, двойственности себе понятия неизотропности) без ограничения общности можно предположить, что 0 не является единственным Θ-пространством, содержащимся в S. Тогда $S^\sigma = S^0$; из конечности ранга F-пространства A и определения подпространства S^0 следует существование конечного числа таких минимальных Θ-пространств $M_1, \ldots, M_k$, принадлежащих S_Θ^τ, что $S^\sigma = S^0 = M_1 \cap \ldots \cap M_k$. Но Θ-пространство M_i тогда и только тогда является минимальным в множестве S_Θ, когда $M_i^\tau = M_i^\sigma$ является максимальным Θ-пространством, содер-

жащимся в S. Отсюда и из условия IV вытекает, что

$$S \cap M_1 = \ldots = S \cap M_k = D.$$

Поэтому

$$0 = S \cap S^\sigma = S \cap M_1 \cap \ldots \cap M_k = (S \cap M_1) \cap \ldots \cap (S \cap M_k) = D.$$

Теперь, поскольку σ является полярным отображением, M_i, как Θ-пространство, неизотропно и $M_i^\sigma \leqslant S$, мы получаем, что

$$S = M_i^\sigma \dotplus (S \cap M_i) = M_i^\sigma.$$

Следовательно, S принадлежит Θ, ибо одновременно с M_i и $M_i^\sigma = M_i^\tau$ является Θ-пространством; этим утверждение (5) полностью доказано.

Из всех полученных результатов следует, что σ является таким полярным отображением F-пространства A, что Θ представляет собой совокупность всех неизотропных относительно σ подпространств и σ на множестве Θ совпадает с заданной перестановкой τ. Таким образом, теорема существования полностью доказана.

Замечание 1. Отметим, что при нашем доказательстве в большей или в меньшей степени были использованы все шесть условий. Вопрос о том, можно ли часть из этих условий опустить, еще не выяснен. Тем не менее, можно указать, что условие VI (а) является независимым, ибо множество Θ, состоящее только из 0 и A, и перестановка τ, переставляющая между собой 0 и A, удовлетворяют всем нашим условиям, кроме VI (а); это условие не выполняется ввиду того, что $r(A) \geqslant 3$.

Замечание 2. Если мы захотим дополнительно потребовать, чтобы σ являлась нуль-системой, то для этого нужно к нашим шести условиям добавить еще условие о том, что Θ не содержит точек и гиперплоскостей.

Замечание 3. Если Θ состоит из всех подпространств F-пространства A, то наши шесть условий будут представлять собой не что иное, как очень громоздкий способ выражения того, что τ является полярным отображением [1]).

Замечание 4. Результаты этого параграфа могут быть использованы при первой попытке охарактеризовать внутренними свойствами группу полярного отображения (§ 5). В самом деле, пусть σ — некоторое полярное отображение, Φ — группа σ-допустимых линейных преобразований (т. е. линейных преобразований, индуцирующих σ-допустимые коллинеации). В силу следствия 1 (§ 5), каждая пара неизотропных подпространств $[U, U^\sigma]$ является

[1]) Относительно такого полярного отображения каждое подпространство будет неизотропным.—*Прим. перев.*

парой подпространств $[J^+(\tau), J^-(\tau)]$ для некоторой инволюции τ первого рода из Φ [1]. Если обозначить через Γ подгруппу группы Φ, порожденную всеми инволюциями первого рода, то, как нетрудно проверить, Φ будет нормализатором подгруппы Γ в группе всех линейных преобразований. Следовательно, если группа Φ линейных преобразований обладает такой системой инволюций, что соответствующие им подпространства J^+, J^- удовлетворяют условиям I — VI и что Φ является нормализатором этой системы во всей группе линейных преобразований, то Φ будет группой всех допустимых линейных преобразований относительно некоторого полярного отображения. Однако это замечание следует рассматривать только как первый шаг в решении задачи охарактеризовать внутренними свойствами группу Φ. В действительности эта задача здесь по существу лишь начинается и сама по себе очень увлекательна. Читатель может ознакомиться с этим вопросом по таким работам, как Дьёдонне [1,2], Хуа Ло-гэн [3], Ван-дер-Варден [1], Вейль [1]. Кроме того, мы можем сослаться на работы Бэра [4], Рикарта [2,3], а также на работы по теоретико-групповым основам эллиптической геометрии, как, например, работы Бэра [5] и Шмидта [1].

---

[1]) Автор, очевидно, предполагает, что характеристика основного тела отлична от 2.—*Прим. перев.*

ГЛАВА V

КОЛЬЦО ЭНДОМОРФИЗМОВ ЛИНЕЙНОГО МНОГООБРАЗИЯ

Быть может, следует осветить сначала общее направление, к которому относятся вопросы, рассматриваемые в настоящей главе. Оно является чрезвычайно ярким примером того, что мы можем назвать *задачей о производных многообразиях*, задачей, которая оказывается интересной для различных областей математики, — так, например, производные многообразия нормированных линейных пространств рассматриваются в работе Макки [1].

Задачу о производных многообразиях можно сформулировать следующим образом. Дан некоторый основной математический объект, и на основе его определен некоторый другой (производный) математический объект. Требуется установить, насколько полно этим производным объектом определяется основной объект и каким образом свойства основного объекта отражаются в свойствах производного объекта. Очень хороший пример такого рода дают линейное многообразие (основной объект) и частично упорядоченное множество его подпространств (производный объект). Из первой основной теоремы проективной геометрии (гл. III, § 1) следует, что если исключить из рассмотрения линейные многообразия малых размерностей, то частично упорядоченное множество подпространств полностью определяет исходное линейное многообразие. Другим примером такого типа является полярное отображение (основной объект) и его группа (производный объект); см. гл. IV, § 5.

Кольцо эндоморфизмов линейного многообразия, к изучению которого мы приступаем, с исчерпывающей полнотой отражает свойства исходного линейного многообразия. Основным орудием исследования в этой главе будет служить «треугольная теория Галуа». С ее помощью устанавливаются очень тесные связи между правыми идеалами кольца, подпространствами линейного многообразия и левыми идеалами кольца; эти связи дают возможность истолковать свойства линейного многообразия на языке свойств кольца эндоморфизмов и обратно. Так, проективные отображения и изоморфизмы кольца, а также дуальные отображения и инверсные изоморфизмы кольца взаимно определяют друг друга.

Изучение тех же вопросов при более общих предположениях читатель может найти в работе Бэра [3].

§ 1. Определение кольца эндоморфизмов

Эндоморфизмом линейного многообразия (F, A) называется однозначное отображение σ F-пространства A в себя, удовлетворяющее следующим условиям:

$(a' + a'')\sigma = a'\sigma + a''\sigma$, $(xa)\sigma = x(a\sigma)$ для a, a', a'' из A и x из F.

(Заметим, что образом элемента a F-пространства A при отображении σ является элемент $a\sigma$ того же пространства A.) Таким образом, эндоморфизмы являются как раз тем, что в теории векторных пространств принято называть особенными и неособенными линейными преобразованиями F-пространства A в себя; линейные преобразования, которые мы рассматривали в предыдущих главах, являются частными случаями эндоморфизмов. С другой стороны, полулинейное преобразование линейного многообразия (F, A) на себя тогда и только тогда является эндоморфизмом, когда оно линейно.

Если σ есть эндоморфизм линейного многообразия (F, A), то совокупность $A\sigma$ элементов вида $a\sigma$ для a из A будет, как легко проверить, подпространством F-пространства A; ранг подпространства $A\sigma$ часто называют *рангом эндоморфизма* σ. Совокупность $K(\sigma)$ всех таких элементов x из A, что $x\sigma = 0$, также является подпространством F-пространства A; ранг этого подпространства часто называют *дефектом эндоморфизма* σ. Мы будем называть подпространство $K(\sigma)$ *ядром эндоморфизма* σ; эндоморфизм является обобщением «проектирования A на $A\sigma$ в направлении ядра $K(\sigma)$»

(1) $A\sigma \sim A/K(\sigma)$.

Этому важному утверждению можно придать следующую более точную формулировку.

(1*) *Эндоморфизм* σ *индуцирует линейное преобразование (в ранее определенном смысле) фактор-пространства* $A/K(\sigma)$ *на подпространство* $A\sigma$.

В справедливости этого утверждения можно легко убедиться, если принять во внимание эквивалентность следующих утверждений: $a \equiv b \pmod{K(\sigma)}$; $a - b$ содержится в $K(\sigma)$; $a\sigma = b\sigma$.

Из утверждения (1) непосредственно следует, что

(2) $r[A\sigma] = r[A/K(\sigma)]$;

из этой формулы и специальной формулы для ранга получаем, что

(3) $r(A) = r[A\sigma] + r[K(\sigma)]$.

Последнее соотношение можно выразить следующими словами: ранг линейного многообразия равен сумме ранга и дефекта каждого его эндоморфизма. Заметим, что формулы (2) и (3) эквивалентны в случае, когда ранг $r(A)$ конечен; в случае же бесконечного ранга $r(A)$ формула (2) является более сильной.

Совокупность всех эндоморфизмов линейного многообразия (F, A) мы обозначим через $\mathrm{P}(F, A)$ [или $\mathrm{P}(A)$, или P]; сложе-

ние и умножение элементов σ', σ'' из P определим следующим образом:

$$a(\sigma'+\sigma'')=a\sigma'+a\sigma'', \quad a(\sigma'\sigma'')=(a\sigma')\sigma'' \text{ для каждого } a \text{ из } A.$$

Нетрудно проверить, что сумма $\sigma'+\sigma''$ и произведение $\sigma'\sigma''$ эндоморфизмов σ', σ'' также являются эндоморфизмами линейного многообразия (F, A). Таким образом, P замкнуто относительно указанных операций. Теперь легко убедиться в том, что P является кольцом; тем самым оправдывается для P (F, A) название *кольцо эндоморфизмов* (или короче — *кольцо*) *линейного многообразия* (F, A). [В старой литературе это кольцо часто называлось кольцом автоморфизмов линейного многообразия (F, A).]

ИДЕМПОТЕНТЫ И ЭНДОМОРФИЗМЫ РАЗЛОЖЕНИЯ

Эндоморфизм σ называется *идемпотентом*, если $\sigma^2=\sigma$. Простыми примерами идемпотентов являются эндоморфизмы 0 и 1, определяемые следующим образом: $a0=0$ и $a1=a$ для каждого a из A.

Если σ — идемпотент, то положим $\sigma'=1-\sigma$. Без труда убеждаемся в том, что

$$\sigma\sigma'=\sigma'\sigma=\sigma-\sigma^2=0 \quad \text{и} \quad \sigma'^2=(1-\sigma)^2=1-2\sigma+\sigma^2=1-\sigma=\sigma',$$

Таким образом, $1-\sigma$ является идемпотентом, «ортогональным» идемпотенту σ; два идемпотента σ и $\sigma'=1-\sigma$ взаимно дополняют друг друга, поскольку $\sigma+\sigma'=1$. Заметим, что идемпотенты ν и ω называются *ортогональными*, если $\nu\omega=\omega\nu=0$.

(4) *Если* σ *— идемпотентный эндоморфизм F-пространства* A, *то*

$$K(\sigma)=A(1-\sigma), \quad A\sigma=K(1-\sigma), \quad A=A\sigma\dot{+}K(\sigma).$$

Это утверждение почти непосредственно следует из очевидной формулы

$$a=a\sigma+a(1-\sigma) \text{ для каждого } a \text{ из } A$$

и из установленных выше свойств ортогональности и идемпотентности эндоморфизмов. Заметим, в частности, что σ оставляет неподвижным каждый элемент из $A\sigma$, а $1-\sigma$ составляет неподвижным каждый элемент из $A(1-\sigma)$. [Таким образом, идемпотентные эндоморфизмы точно эквивалентны тому, что часто называют проектированием A на $A\sigma$ в направлении $K(\sigma)$.]

(5) *Если* $\sigma_1, \ldots, \sigma_n$ *— конечное множество попарно ортогональных идемпотентов и если*

$$1=\sum_{i=1}^{n}\sigma_i, \quad \text{то} \quad A=A\sigma_1\dot{+}\ \ldots\ \dot{+}A\sigma_n.$$

Доказательство. Идемпотенты σ_i удовлетворяют условию

$$\sigma_i \sigma_j = \begin{cases} \sigma_i \text{ для } i = j, \\ 0 \text{ для } i \neq j. \end{cases}$$

Так как I представима в виде суммы этих идемпотентов σ_i, то

(5.1) $a = a\sigma_1 + \ldots + a\sigma_n$ для каждого a из A.

Если, в частности, $0 = \sum_{i=1}^{n} a_i$, где $a_i \in A\sigma_i$, то $a_i = b_i\sigma_i$ и, следовательно,

$$a_i\sigma_j = b_i\sigma_i\sigma_j = \begin{cases} b_i\sigma_i = a_i \text{ для } i = j, \\ b_i 0 = 0 \text{ для } i \neq j. \end{cases}$$

Поэтому, действуя на левую и правую части нашего равенства эндоморфизмом σ_i, мы получаем, что $0 = 0\sigma_i = a_i$. Таким образом:

(5.2) Из $0 = a_1 + \ldots + a_n$, где $a_i \in A\sigma_i$, следует $a_1 = \ldots = a_n = 0$.

Но утверждения (5.1) и (5.2) вместе и означают справедливость предложения (5).

Обратно, если $A = A_1 \dotplus \ldots \dotplus A_n$, то обозначим через σ_i однозначно определенный эндоморфизм F-пространства A, оставляющий неподвижным каждый элемент из A_i и отображающий все элементы из $\sum_{j \neq i} A_j$ на 0. Легко проверить, что σ_i будут попарно ортогональными идемпотентами, сумма которых равна 1, и что $A_i = A\sigma_i$. Эти идемпотенты называются (*дополнительными*) *эндоморфизмами разложения, принадлежащими данному прямому разложению F-пространства A*. Из этого замечания и предложения (5) вытекает, что «прямое разложение линейного многообразия в конечное число компонент» и «конечное множество попарно ортогональных идемпотентов, сумма которых равна 1», являются эквивалентными понятиями, поскольку такие прямые разложения и такие конечные множества идемпотентов взаимно однозначно определяют друг друга.

Если дано прямое разложение F-пространства A в бесконечное множество слагаемых A_ν, то также можно определить эндоморфизмы разложения σ_ν; σ_ν оставляет неподвижным каждый элемент из A_ν и аннулирует все элементы из остальных компонент. Также легко проверяется, что σ_ν являются попарно ортогональными идемпотентами; но мы не можем утверждать, что сумма этих идемпотентов равна 1, поскольку сумма бесконечного множества слагаемых в кольце P вообще не определена. Однако имеются различные способы для преодоления этого затруднения. Один из них основывается на том, что, как можно показать, σ_ν образуют максимальную систему попарно ортогональных идемпотентов. Можно пойти и по другому пути, используя то, что для каждого элемента a из A существует лишь конечное число эндоморфизмов

разложения σ_ν, не отображающих a на 0; на основании этого утверждения становится возможным разумным образом определить сумму бесконечного множества слагаемых σ_ν. [Дополнительные детали, относящиеся к этому вопросу, читатель может найти, например, в работе Бэра [1].]

ПРЕДСТАВЛЕНИЕ КОЛЬЦА ЭНДОМОРФИЗМОВ МАТРИЦАМИ

Такое представление поможет читателю связать введенные нами понятия с хорошо известными ему понятиями. Однако само это представление будет мало использовано в последующих рассмотрениях.

Пусть (F, A) — линейное многообразие конечного ранга n. Выберем некоторый его базис B, состоящий из элементов $b_1, \ldots, b_n$; B мы будем рассматривать как упорядоченное множество элементов. Если σ есть эндоморфизм F-пространства A, то

$$b_i \sigma = \sum_{j=1}^{n} b_{ij} b_j \text{ для } i = 1, \ldots, n;$$

таким образом, эндоморфизм σ можно отобразить на однозначно определенную $n \times n$-матрицу $\sigma^B = (b_{ij})$ (индексы i и j указывают соответственно строку и столбец, в которых расположен элемент b_{ij}). Необходимо заметить, что так определенное отображение существенно зависит от выбора базиса B и что оно изменяется даже от перестановки элементов множества B.

Из формулы

$$\Big[\sum_{i=1}^{n} x_i b_i\Big] \sigma = \sum_{i=1}^{n} x_i \sum_{j=1}^{n} b_{ij} b_j = \sum_{j=1}^{n} \Big[\sum_{i=1}^{n} x_i b_{ij}\Big] b_j \qquad (\Pi)$$

видно, что эндоморфизм σ полностью определяется соответствующей ему матрицей σ^B. Таким образом, отображение $\sigma \longrightarrow \sigma^B$ является взаимно однозначным. Если прочесть формулу (П) справа налево, то можно увидеть, как произвольно заданная матрица (b_{ij}) определяет такой эндоморфизм σ, что $\sigma^B = (b_{ij})$; отсюда следует, что отображение $\sigma \longrightarrow \sigma^B$ является взаимно однозначным отображением кольца P на совокупность F_n всех $n \times n$-матриц с коэффициентами из тела F.

В F_n можно обычным образом определить сложение и умножение:

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}), \quad (a_{ij})(b_{ij}) = \Big(\sum_{k=1}^{n} a_{ik} b_{kj}\Big).$$

Используя эти определения, читатель легко сможет убедиться в справедливости равенств

$$\sigma'^B + \sigma''^B = (\sigma' + \sigma'')^B, \quad \sigma'^B \sigma''^B = (\sigma' \sigma'')^B,$$

из которых следует, что наше отображение кольца P на кольцо матриц F_n является изоморфным.

Если B' и B'' – базисы F-пространства A, то соответствия $\sigma \longrightarrow \sigma^{B'}$ и $\sigma \longrightarrow \sigma^{B''}$ задают изоморфные отображения кольца P на кольцо матриц F_n. Мы предоставляем читателю доказать, что эти два изоморфных отображения отличаются друг от друга лишь на внутренний автоморфизм кольца F_n, индуцированный той матрицей из F_n, которая переводит один из базисов B', B'' в другой.

Если линейное многообразие (F, A) имеет бесконечный ранг, то можно провести очень похожие рассмотрения. Однако в этом случае нужно рассматривать совокупность не всех матриц, а лишь таких, у которых в каждой строке только конечное число элементов отлично от 0. Кроме того, определенное внимание нужно уделить рассмотрению всевозможных упорядочений данного базиса, порядковые типы которых могут быть существенно различными.

§ 2. Треугольная теория Галуа

Так как кольцо эндоморфизмов P линейного многообразия (F, A) обладает единичным элементом 1, то *правые идеалы кольца* P можно определить как его непустые подмножества J, удовлетворяющие условиям

$$J = J \pm J = J\mathrm{P};$$

аналогично, *левыми идеалами кольца* P называются его непустые подмножества H, удовлетворяющие условиям

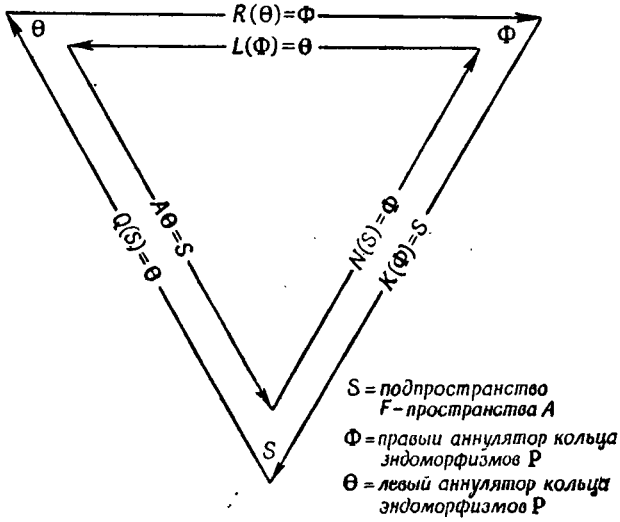
$$H = H \pm H = \mathrm{P}H.$$

Таким образом, правые, так же как и левые, идеалы содержат суммы и разности своих элементов (и замкнуты относительно умножения). Кроме того, правый идеал вместе с любым своим элементом j содержит все элементы jj', получающиеся при умножении j на произвольный элемент j' из P справа; аналогично, левый идеал вместе с каждым своим элементом содержит все элементы, получающиеся при умножении этого элемента на любой элемент кольца P слева.

Если S – произвольное подмножество кольца P, то совокупность $L(S)$ таких элементов x из P, что $xS = 0$, является, очевидно, левым идеалом; такой левый идеал мы будем называть *левым аннулятором*, а именно левым аннулятором, определенным множеством S. Аналогично, обозначим через $R(S)$ совокупность таких элементов y кольца P, что $Sy = 0$. Очевидно, что $R(S)$ является правым идеалом; такой правый идеал мы будем называть

правым аннулятором, а именно правым аннулятором, определенным подмножеством S. (Вопрос о том, при каких условиях каждый идеал [1]) является аннулятором, мы разберем в следующем параграфе.)

Треугольная теория Галуа, которой посвящается настоящий параграф, состоит в построении проективного соответствия между подпространствами F-пространства A и левыми аннуляторами кольца P, а также дуальных соответствий между подпространствами F-пространства A и правыми аннуляторами кольца P и между правыми и левыми аннуляторами [2]).



Фиг. 12.

Для того, чтобы получить эти соответствия, нам нужно, кроме уже определенных операторов L и R, определить еще *четыре оператора*.

Если S есть подмножество F-пространства A, то через $N(S)$ обозначим совокупность всех таких элементов σ кольца эндоморфизмов P, что $S\sigma = 0$, а через $Q(S)$ – совокупность таких элементов σ из P, что $A\sigma \leqslant S$. Нетрудно проверить, что $N(S)$ является правым идеалом кольца P; $Q(S)$ будет левым идеалом, если только S замкнуто относительно сложения. Правый идеал $N(S)$ можно назвать аннулятором множества S; совокупность $Q(S)$

[1]) Под идеалом автор понимает произвольный левый или правый идеал; аналогичную терминологию автор употребляет и для аннуляторов. — *Прим. перев.*

[2]) Определения проективного и дуального отображений одного частично упорядоченного множества на другое см. в добавлении М. — *Прим. перев.*

является в некотором роде частным S по A — так, если S есть подпространство F-пространства A, то $Q(S)$ в точности аннулирует фактор-пространство A/S.

Если J — подмножество кольца P, то через $K(J)$ обозначим совокупность всех таких элементов x из A, что $xJ=0$ (т. е. $x\sigma=0$ для каждого σ из J). Легко убедиться, что это ядро $K(J)$ множества J является подпространством F-пространства A. Через AJ обозначим множество всех элементов вида aj для a из A и j из J; заметим, что в общем случае AJ не является подпространством F-пространства A. В связи с этим возникают некоторые трудности; однако при естественных ограничениях AJ все же будет подпространством (см. ниже следствие 1, § 3).

Мы можем теперь следующим образом сформулировать основное содержание «треугольной теории Галуа».

Теорема А. *Операторы $N(S)$ и $K(\Phi)$ устанавливают взаимно обратные дуальные соответствия между подпространствами S F-пространства A и правыми аннуляторами Φ кольца эндоморфизмов* P.

Теорема Б. *Операторы $Q(S)$ и $A\Theta$ устанавливают взаимно обратные проективные соответствия между подпространствами S F-пространства A и левыми аннуляторами Θ кольца эндоморфизмов* P.

Теорема В. *Операторы $L(\Phi)$ и $R(\Theta)$ устанавливают взаимно обратные дуальные соответствия между правыми аннуляторами Φ и левыми аннуляторами Θ кольца* P.

Доказательство этих трех теорем будет проведено в несколько этапов. В процессе доказательства мы получим ряд утверждений, дополняющих эту теорию.

Предложение 1. *$K[N(S)]=S=AQ(S)$ для каждого подпространства S F-пространства A.*

Доказательство. По определению оператора $N(S)$, $SN(S)=0$; отсюда и из определения оператора K следует, что $S\leqslant K[N(S)]$. Для доказательства того, что в действительности здесь имеет место равенство, рассмотрим произвольный элемент w F-пространства A, не принадлежащий S. Тогда минимальное подпространство, содержащее S и w, можно представить в виде $S\dotplus Fw$; из теоремы о дополнении (гл. II, § 1) следует существование такого подпространства W, что $A=S\dotplus Fw\dotplus W$. В таком случае существует, и притом только один, такой эндоморфизм σ, что $S\sigma=0$ и $x\sigma=x$ для каждого x из $Fw\dotplus W$ [σ является одним из эндоморфизмов разложения, принадлежащих прямому разложению $A=S\dotplus(Fw\dotplus W)$]. Очевидно, что σ содержится в $N(S)$ и, поскольку $w\sigma=w$ и $w\neq 0$, элемент w не принадлежит $K[N(S)]$. Таким образом, S не меньше $K[N(S)]$ и, следовательно, $S=K[N(S)]$.

Из определения оператора Q вытекает, что $AQ(S) \leqslant S$. Рассмотрим теперь произвольный элемент s, принадлежащий S. Так как Fs является подпространством F-пространства A, то, в силу принципа дополнения, в A существует такое подпространство T, что $A = Fs + T$. Существует такой однозначно определенный эндоморфизм τ F-пространства A, при котором $s\tau = s$ и $T\tau = 0$; этот эндоморфизм удовлетворяет условию $A\tau = Fs \leqslant S$. Следовательно, τ содержится в $Q(S)$, а s содержится в $AQ(S)$. Тем самым мы установили, что $S \leqslant AQ(S) \leqslant S$, откуда $S = AQ(S)$, что и требовалось доказать.

Предложение 2. *$N(AJ) = R(J)$ и $Q[K(J)] = L(J)$ для каждого подмножества J кольца* P.

В справедливости этого предложения легко убедиться, используя достаточно очевидную эквивалентность следующих утверждений:

σ принадлежит $R(J)$; $J\sigma = 0$; $AJ\sigma = 0$; σ принадлежит $N(AJ)$

и эквивалентность следующих утверждений:

σ принадлежит $L(J)$; $\sigma J = 0$; $A\sigma J = 0$; $A\sigma \leqslant K(J)$;

σ принадлежит $Q[K(J)]$.

Из предложений 1 и 2 следует, что

$$N(S) = N[AQ(S)] = R[Q(S)]; \quad Q(S) = Q[K(N(S))] = L[N(S)]$$

для каждого подпространства S F-пространства A, т. е. справедливо

Предложение 3. *$N(S) = R[Q(S)]$ и $Q(S) = L[N(S)]$ для каждого подпространства S F-пространства A.*

Замечание 1. Предложение 3 является своего рода уточнением важного легко доказываемого соотношения:

$$Q(S)N(S) = 0$$

для каждого подмножества S F-пространства A.

Предложение 4. *$J = Q(AJ)$ для каждого левого аннулятора J из* P *и $H = N[K(H)]$ для каждого правого аннулятора H из* P.

Доказательство. Так как J есть левый аннулятор, то $J = L(T)$, где T — некоторое подмножество кольца P. Отсюда, в силу предложений 1 и 2,

$$J = L(T) = Q[K(T)], \; AJ = AQ[K(T)] = K(T), \; Q(AJ) = Q[K(T)] = J.$$

Так как H — правый аннулятор, то $H = R(M)$ для некоторого подмножества M кольца P. Подмножество AM F-пространства A порождает некоторое подпространство S. Легко проверить, что

$N(AM)=N(S)$; отсюда и из предложений 1 и 2 вытекает, что

$$H=R(M)=N(AM)=N(S),\ K(H)=K[N(S)]=S,$$

$$N[K(H)]=N(S)=H,$$

и этим предложение 4 полностью доказано.

Доказательство теоремы А. В силу предложений 1, 3 и 4,

$$S=K[N(S)],\ N(S)=R[Q(S)]$$

для каждого подпространства S F-пространства A,

$$H=N[K(H)]$$

для каждого правого аннулятора H из P. Из этих равенств видно, что оператор $K(H)$, определенный на правых аннуляторах H кольца P, и оператор $N(S)$, определенный на подпространствах S F-пространства A, устанавливают взаимно обратные соответствия между системой всех подпространств линейного многообразия (F, A) и системой всех правых аннуляторов из кольца эндоморфизмов P. Отсюда, в частности, следует, что каждый из операторов K и N определяет взаимно однозначное отображение одной из указанных систем на всю другую.

Если S и T – такие подпространства F-пространства A, что $S\leqslant T$, то $N(T)\leqslant N(S)$; аналогично, если H, J – подмножества кольца P и $H\leqslant J$, то $K(J)\leqslant K(H)$; оба эти соотношения непосредственно вытекают из определений операторов N и K. Следовательно, K и N являются взаимно обратными дуальными соответствиями между системой всех подпространств F-пространства A и системой всех правых аннуляторов из кольца P.

Доказательство теоремы Б. В силу предложений 1, 3 и 4,

$$S=AQ(S),\ Q(S)=L[N(S)]$$

для каждого подпространства S F-пространства A,

$$J=Q(AJ)$$

для каждого левого аннулятора J из P. Теперь легко проверить (подобно тому, как это было сделано при доказательстве теоремы А), что отображения S на $Q(S)$ и J на AJ являются взаимно обратными проективными соответствиями между системой всех подпространств F-пространства A и системой всех левых аннуляторов из кольца P [1]).

Замечание 2. Теорема Б показывает, что левые аннуляторы из кольца эндоморфизмов P составляют точное представление проективной геометрии всех подпространств F-пространства A. Для того, чтобы этим представлением можно было бы

[1]) То, что AJ является подпространством, если J есть левый аннулятор, следует из доказательства предложения 4. — *Прим. перев.*

пользоваться, необходимо дать внутреннюю характеристику аннуляторов; см. в связи с этим следующий параграф.

Доказательство теоремы B. Если J – левый аннулятор, то AJ является подпространством F-пространства A (см. доказательство предложения 4); отсюда и из предложений 2, 3 и 4 следует, что

$$L[R(J)] = L[N(AJ)] = Q(AJ) = J;$$

аналогично, для каждого правого аннулятора H мы имеем

$$R[L(H)] = R[Q(K[H])] = N[K(H)] = H.$$

Теперь уже почти очевидно, что L и R являются взаимно обратными дуальными соответствиями между системой всех левых аннуляторов и системой всех правых аннуляторов кольца P.

Замечание 3. Легко видеть, что пересечение любого числа правых аннуляторов является правым аннулятором; аналогичное утверждение справедливо и для левых аннуляторов. Иначе обстоит дело с суммами аннуляторов. В следующем параграфе будет показано, что сумма конечного числа аннуляторов также является аннулятором и что аналогичное утверждение для бесконечного множества аннуляторов, вообще говоря, неверно.

Связь между линейным многообразием и кольцом его эндоморфизмов не ограничивается теми соотношениями, которые выражены в предыдущих результатах. Мы сейчас покажем, что само линейное многообразие можно вложить в его кольцо эндоморфизмов. Одновременно мы покажем, что это кольцо содержит также и сопряженное пространство. С этой целью напомним некоторые из предыдущих результатов.

Если (F, A) – линейное многообразие, то сопряженное ему пространство будем обозначать через A^*. Это пространство мы ввели в § 3 гл. II как пространство всех линейных форм над A [в § 3 гл. II сопряженное пространство обозначалось через $L(A)$; в настоящем параграфе мы пользуемся обозначением A^*, чтобы избежать путаницы с введенным нами оператором L]. Поскольку элементы из A^* умножаются на элементы тела F справа, мы будем сопряженное пространство иногда называть линейным многообразием (A^*, F). Если $a \in A$ и $b \in A^*$, то результат действия линейной формы b на элемент a записывается в виде ab; ab является элементом тела F. Таким образом, всю конфигурацию, состоящую из F-пространства A, тела F и сопряженного пространства A^*, мы можем обозначить через (A^*, F, A). Напомним, кроме того, что $E(T)$ для $T \leqslant A$ состоит из всех таких элементов b из A^*, что $Tb = 0$, а $S(T)$ для $T \leqslant A^*$ состоит из всех таких элементов a из A, что $aT = 0$.

Предложение 5. *Пусть $A = P \cdot H$, где P – точка и H гиперплоскость линейного многообразия (F, A). Тогда существуют*

изоморфное отображение ν *тела* F *на подтело* $N(H) \cap Q(P)$ *кольца* $\mathrm{P}(F, A)$, *изоморфное отображение* α *аддитивной группы* A *на подгруппу* $N(H)$ *и изоморфное отображение* α^* *аддитивной группы* A^* *на подгруппу* $Q(P)$ (*аддитивной группы кольца* P), *обладающие следующими свойствами:*

(а) $(bx)^{\alpha^*} = b^{\alpha^*} x^\nu$, $(xa)^\alpha = x^\nu a^\alpha$, $(ab)^\nu = a^\alpha b^{\alpha^*}$ *для* b *из* A^*, x *из* F *и* a *из* A.

(б) $S^\alpha = Q(S) \cap N(H)$ *и* $E(S)^{\alpha^*} = N(S) \cap Q(P)$ *для каждого подпространства* S F-*пространства* A.

Доказательство. Так как P является точкой, то $P = Fp$; изоморфные отображения, которые мы построим, существенно зависят от выбора элемента p.

Для каждого элемента x тела F существует, и притом только один, эндоморфизм x^ν F-пространства A, обладающий следующими свойствами:

$$px^\nu = xp, \quad Hx^\nu = 0.$$

Достаточно ясно, что ν является взаимно однозначным отображением тела F на подкольцо $N(H) \cap Q(P)$, сохраняющим сумму. Это отображение сохраняет также произведение, так как

$$p(xy)^\nu = xyp = x(yp) = x(py^\nu) = (xp)\, y^\nu = (px^\nu)\, y^\nu = p(x^\nu y^\nu);$$

таким образом, ν представляет собой изоморфное отображение тела F на подкольцо $N(H) \cap Q(P)$ кольца P, и, следовательно, $N(H) \cap Q(P)$ является подтелом кольца P.

Для каждого элемента a F-пространства A существует один и только один эндоморфизм a^α линейного многообразия (F, A), обладающий следующими свойствами:

$$pa^\alpha = a, \quad Ha^\alpha = 0.$$

Очевидно, что α является взаимно однозначным и сохраняющим сложение отображением аддитивной группы A на $N(H)$ [так как всякий эндоморфизм F-пространства A, аннулирующий гиперплоскость H, полностью определяется своим значением на элементе p, а потому на точке P]. Равенство $S^\alpha = Q(S) \cap N(H)$ для подпространств S F-пространства A почти непосредственно следует из того, что $A^\alpha = N(H)$. Если $x \in F$ и $a \in A$, то

$$p(xa)^\alpha = xa = x(pa^\alpha) = (xp)\, a^\alpha = (px^\nu)\, a^\alpha = p(x^\nu a^\alpha), \text{ т. е. } (xa)^\alpha = x^\nu a^\alpha.$$

Если b – элемент сопряженного пространства A^*, то b является линейной формой над A; однозначное отображение b^{α^*} F-пространства A в подпространство P определим следующим образом:

$$ab^{\alpha^*} = (ab)\, p \quad \text{для каждого } a \text{ из } A.$$

Так как $(a' + a'')\, b = a'b + a''b$ и $(xa)\, b = x(ab)$, то b^{α^*} будет эндоморфизмом, содержащимся в $Q(P)$. Также легко проверить, что α^*

является взаимно однозначным и сохраняющим сложение отображением аддитивной группы A^* в аддитивную группу $Q(P)$. Если η — произвольный эндоморфизм из $Q(P)$, то для каждого a из A существует одно и только одно такое число a' из F, что $a\eta = a'p$; нетрудно убедиться, что отображением a на a' задается линейная форма b над A, удовлетворяющая условию $b^{\alpha^*} = \eta$. Таким образом, α^* является изоморфным отображением аддитивной группы A^* на всю подгруппу $Q(P)$ аддитивной группы кольца P. Далее,

$$p(ab)^{\nu} = (ab)p = ab^{\alpha^*} = (pa^{\alpha})b^{\tau^*} = p(a^{\alpha}b^{\tau^*}), \text{ откуда } (ab)^{\nu} = a^{\alpha}b^{\alpha^*};$$

$$a(bx)^{\alpha^*} = [a(bx)]p = (ab)(xp) = (ab)(px^{\nu}) =$$

$$= [(ab)p]x^{\nu} = (ab^{\tau^*})x^{\nu} = a(b^{\alpha^*}x^{\nu})$$

для каждого a из A, b из A^* и x из F, так что $(bx)^{\alpha^*} = b^{\alpha^*}x^{\nu}$. Тем самым показано, что наши изоморфные отображения удовлетворяют всем требованиям условия (а). Последнее требование условия (б), т. е. равенство $E(S)^{\tau^*} = N(S) \cap Q(P)$, почти непосредственно вытекает из эквивалентности следующих свойств элемента b сопряженного пространства A^*:

$$b \text{ принадлежит } E(S);\ 0 = Sb;\ 0 = (Sb)p = Sb^{\alpha^*};$$

$$b^{\tau^*} \text{ принадлежит } N(S),$$

и из того, что $A^{*\alpha^*} = Q(P)$. Таким образом, предложение 5 полностью доказано.

Замечание 4. В предложении 5 содержатся следующие утверждения:

Пара (ν, α) является полулинейным преобразованием линейного многообразия (F, A) на линейное многообразие $[N(H) \cap Q(P), N(H)]$.

Пара (α^*, ν) является полулинейным преобразованием линейного многообразия (A^*, F) на линейное многообразие $[Q(P), N(H) \cap Q(P)]$.

Комбинируя эти утверждения с третьим равенством (а), мы с полным основанием можем высказать (очевидным образом обобщая принятую нами терминологию) следующее утверждение:

Тройка (α^*, ν, α) является полулинейным преобразованием линейной конфигурации (A^*, F, A) на линейную конфигурацию

$$[Q(P), N(H) \cap Q(P), N(H)].$$

§ 3. Идеалы, порожденные конечным множеством элементов

Следующая теорема дает внутреннюю характеристику аннуляторов кольца эндоморфизмов P.

Теорема 1. *Идеал кольца* P *тогда и только тогда будет аннулятором, когда он порождается конечным множеством элементов.*

Доказательство будет разбито на несколько этапов, причем в процессе доказательства мы получим более сильные результаты, чем тот, который сформулирован в теореме.

Предложение 1. *Каждый аннулятор порождается идемпотентом.*

Доказательство. Если J — правый аннулятор, то мы докажем существование такого идемпотента σ, что $J = \sigma P$; аналогично, если J — левый аннулятор, то будет доказано существование такого идемпотента σ, что $J = P\sigma$.

Пусть сначала J будет левым аннулятором. Тогда, по теореме Б (§ 2), существует, и притом только одно, такое подпространство S линейного многообразия (F, A), что $J = Q(S)$. Так как каждое подпространство F-пространства A является в A прямым слагаемым (принцип дополнения), то существует такой идемпотент σ, при котором $A\sigma = S$. Очевидно, что σ содержится в $Q(S) = J$. Следовательно, $P\sigma \leqslant Q(S)$, так как $Q(S)$ — левый идеал. Обратно, если эндоморфизм τ принадлежит $Q(S)$, то $A\tau < S$. Таким образом, $a\tau$ содержится в S для каждого a из A; следовательно, $a\tau = a\tau\sigma$, ибо идемпотент σ оставляет неподвижным каждый элемент подпространства $S = A\sigma$. Этим показано, что $\tau = \tau\sigma$, т. е. τ содержится в $P\sigma$. Тем самым $P\sigma = Q(S) = J$, что и требовалось доказать.

Пусть теперь J — правый аннулятор. В этом случае, в силу теоремы А (§ 2), существует одно и только одно такое подпространство T F-пространства A, что $J = N(T)$. Снова используя то обстоятельство, что каждое подпространство является прямым слагаемым всего пространства, мы найдем такой идемпотентный эндоморфизм σ F-пространства A, для которого $T = K(\sigma)$. Очевидно, что σ принадлежит $N(T)$ и, поскольку $N(T)$ — правый идеал, $\sigma P \leqslant N(T)$. Пусть теперь τ — произвольный эндоморфизм из $N(T)$. Каждый элемент a F-пространства A можно представить в виде $a = a\sigma + a(1-\sigma)$; при этом $a(1-\sigma)$ принадлежит $K(\sigma) = T$, поскольку σ является идемпотентом. Следовательно, $a(1-\sigma)\tau = 0$, откуда $a\tau = a\sigma\tau$, т. е. $\tau = \sigma\tau$. Таким образом, τ содержится в σP, и тем самым $\sigma P = N(T) = J$; этим предложение 1 полностью доказано.

Лемма 1. *Для каждого эндоморфизма σ F-пространства A существует такой эндоморфизм η того же пространства, что*

(а) *эндоморфизмы $\sigma\eta$ и $\eta\sigma$ являются идемпотентами;*

(б) $A\sigma = A\eta\sigma$, $K(\eta) = K(\eta\sigma)$, $K(\sigma\eta) = K(\sigma)$, $A\sigma\eta = A\eta$.

Доказательство. Так как $A\sigma$ и $K(\sigma)$ являются подпространствами F-пространства A, то, в силу принципа дополнения, существуют такие подпространства S и T, что

$$A = A\sigma \dotplus S = T \dotplus K(\sigma).$$

Если x и y — такие элементы из T, что $x\sigma = y\sigma$, то $x - y$ принад-

лежит пересечению подпространств T и $K(\sigma)$, которое равно 0; таким образом, $x = y$. Следовательно, σ индуцирует линейное преобразование подпространства T на подпространство $T\sigma = T\sigma + K(\sigma)\sigma = A\sigma$. Такое преобразование обладает обратным преобразованием τ; заметим, что τ является линейным преобразованием подпространства $A\sigma$ на подпространство T, удовлетворяющим условиям: $x\sigma\tau = x$ для каждого x из T и $y\tau\sigma = y$ для каждого y из $A\sigma$. Так как $A = A\sigma \dotplus S$, то существует, и притом только один, эндоморфизм η F-пространства A, индуцирующий на $A\sigma$ отображение τ и аннулирующий подпространство S. Таким образом, для произвольных a из T и s из S мы имеем

$$(a\sigma + s)\eta = a\sigma\tau = a;$$

заметим, что в виде $a\sigma + s$ можно представить каждый элемент F-пространства A, поскольку $T\sigma = A\sigma$. Из полученного равенства вытекает, что $K(\eta) = S$ и $A\eta = T$. Если, в частности, в этом равенстве мы положим $s = 0$, то найдем, что

$$a(\sigma\eta) = a \text{ и } (a\sigma)\eta\sigma = a\sigma \text{ для каждого } a \text{ из } T.$$

Так как $K(\sigma) \leqslant K(\sigma\eta)$, то из первого равенства следует, что $\sigma\eta$ является таким идемпотентным эндоморфизмом, что $A\sigma\eta = T$ и $K(\sigma\eta) = K(\sigma)$; аналогично, поскольку $S \leqslant K(\eta\sigma)$, второе равенство показывает, что $\eta\sigma$ является таким идемпотентным эндоморфизмом, что $A\eta\sigma = T\sigma = A\sigma$ и $K(\eta\sigma) = S$.

Предложение 2. *Для каждого эндоморфизма σ линейного многообразия (F, A) существует такой эндоморфизм σ', что $\sigma = \sigma\sigma'\sigma$.*

Кольца, обладающие сформулированным в этом предложении свойством, часто называют *регулярными*.

Доказательство. В силу леммы 1, существует такой эндоморфизм σ' F-пространства A, что $\sigma'\sigma$ будет идемпотентом и $A\sigma'\sigma = A\sigma$. Таким образом, идемпотент $\sigma'\sigma$ оставляет неподвижным каждый элемент подпространства $A\sigma'\sigma = A\sigma$ и, следовательно, $a\sigma = a\sigma\sigma'\sigma$ для любого a из A, т. е. $\sigma = \sigma\sigma'\sigma$.

Предложение 3. *Сумма конечного множества аннуляторов является аннулятором.*

Доказательство. Достаточно, очевидно, доказать, что сумма двух аннуляторов будет аннулятором. Предположим сначала, что J' и J'' - левые аннуляторы. Тогда, в силу предложения 1, существуют такие идемпотенты σ' и σ'', что $J' = P\sigma'$ и $J'' = P\sigma''$. Дважды используя принцип дополнения, мы найдем такие подпространства S и T, что

$$A\sigma'' = (A\sigma' \cap A\sigma'') \dotplus S, \quad A = (A\sigma' + A\sigma'') \dotplus T,$$

откуда

$$A\sigma' + A\sigma'' = A\sigma' \dotplus S, \quad A = A\sigma' \dotplus S \dotplus T.$$

Используя последнее разложение F-пространства A, можно легко построить идемпотентные эндоморфизмы η', η'', обладающие следующими свойствами:

$$A\eta' = A\sigma',\ K(\eta') = S + T;\ A\eta'' = S,\ K(\eta'') = A\sigma' + T.$$

Нетрудно проверить, что эти идемпотенты удовлетворяют соотношениям

$$\eta'\eta'' = \eta''\eta' = 0,\ \eta' = \eta'\sigma',\ \sigma' = \sigma'\eta',\ \eta'' = \eta''\sigma'',$$

из которых вытекает, что η' содержится в J', η'' содержится в J'' и, следовательно, $\eta = \eta' + \eta''$ содержится в $J' + J''$. Далее, простым подсчетом можно убедиться, что сумма η двух ортогональных идемпотентов также является идемпотентом. Левый идеал $P\eta$, несомненно, содержит $\sigma' = \sigma'\eta' = \sigma'\eta'\eta$. Так как

$$A\sigma'' \leqslant A\sigma' + A\sigma'' = A\sigma' \dotplus S = A\eta' \dotplus A\eta'' = A\eta$$

и η является идемпотентом, то $\sigma'' = \sigma''\eta$. Таким образом, $P\eta$ содержит оба идемпотента σ' и σ''. Отсюда следует, что $J' + J'' = P\eta$, а так как η — идемпотент, то $P\eta = L(1-\eta)$. Тем самым показано, что сумма двух (и, следовательно, произвольного конечного числа) левых аннуляторов является левым аннулятором.

Пусть теперь J' и J'' — правые аннуляторы. Тогда, в силу предложения 1, существуют такие идемпотенты σ', σ'', что $J' = \sigma' P$ и $J'' = \sigma'' P$. Заметим, что $K(\sigma', \sigma'') = K(\sigma') \cap K(\sigma'')$. Теперь воспользуемся принципом дополнения, в силу которого существуют такие подпространства S', S'', T, что

$$K(\sigma') = K(\sigma', \sigma'') \dotplus S',\ K(\sigma'') = K(\sigma', \sigma'') \dotplus S'',\ A = T + [K(\sigma') + K(\sigma'')]$$

и, следовательно,

$$K(\sigma') + K(\sigma'') = S' + S'' \dotplus K(\sigma', \sigma''),\ A = T \dotplus S' \dotplus S'' \dotplus K(\sigma', \sigma'').$$

Отсюда ясно, как можно построить идемпотентные эндоморфизмы η', η'' F-пространства A, удовлетворяющие условиям

$$A\eta' = S'',\ K(\eta') = T + K(\sigma'),\ A\eta'' = S' + T,\ K(\eta'') = K(\sigma'').$$

Так как $A\eta' \leqslant K(\eta'')$ и $A\eta'' \leqslant K(\eta')$, то $\eta'\eta'' = \eta''\eta' = 0$; поэтому сумма $\eta = \eta' + \eta''$ этих ортогональных идемпотентов сама является идемпотентом. Далее, из $A = A\eta' \dotplus A\eta'' \dotplus K(\sigma', \sigma'')$ легко следует, что $K(\eta) = K(\sigma', \sigma'')$. Теперь заметим, что для каждого идемпотента σ справедливо равенство $\sigma P = R(1-\sigma)$. Поэтому мы можем воспользоваться теоремой A (§ 2), из которой вытекает, что $\sigma P = N[K(\sigma P)] = N[K(\sigma)]$. Таким образом, правый идеал σP состоит из всех эндоморфизмов $\varkappa$, удовлетворяющих условию $K(\sigma) \leqslant K(\varkappa)$.

Из этого замечания и из включений

$$K(\eta) \leqslant K(\sigma') \leqslant K(\eta'),\ K(\eta) \leqslant K(\sigma'') \leqslant K(\eta'')$$

следует, что ηP содержит σ' и σ'', $J' = \sigma'$P содержит η' и $J'' = \sigma''$P содержит η''. Таким образом, $\eta = \eta' + \eta''$ содержится в $J' + J'' = \sigma'$P $+ \sigma''$P $\leqslant \eta$P, и этим показано, что $J' + J'' = \eta$P $= R(1-\eta)$. Тем самым сумма двух (и, следовательно, произвольного конечного числа) правых аннуляторов является правым аннулятором.

Доказательство теоремы 1. Согласно предложению 1, каждый аннулятор порождается одним своим идемпотентом, так что он тем более является идеалом, порожденным конечным множеством элементов. Обратно, пусть левый идеал J порождается конечным множеством элементов; иными словами, существует такое конечное множество элементов $j_1, \ldots, j_n$, что J является минимальным левым идеалом, содержащим все эти элементы. Обозначим через J_i главный левый идеал, порожденный элементом j_i. Тогда $J = \sum_{i=1}^{n} J_i$. Из предложения 2 следует существование таких элементов j_i', что $j_i = j_i j_i' j_i$. Эндоморфизм $\sigma_i = j_i' j_i$ будет, очевидно, идемпотентом, содержащимся в J_i. Так как элемент $j_i = j_i \sigma_i$ принадлежит Pσ_i, то $J_i =$ Pσ_i. Принимая теперь во внимание, что σ_i является идемпотентом, мы получаем, что $J_i =$ P$\sigma_i = L(1-\sigma_i)$; таким образом, J_i является левым аннулятором. Отсюда и из предложения 3 вытекает, что левый идеал J, как сумма конечного числа левых аннуляторов, сам будет левым аннулятором. Подобным же образом доказывается, что правый идеал кольца эндоморфизмов P, порожденный конечным множеством элементов, является правым аннулятором.

Следствие 1. *AJ является подпространством F-пространства A для каждого левого идеала J кольца эндоморфизмов* P.

Доказательство. Любые два элемента из AJ можно представить в виде $a'j'$ и $a''j''$, где a', a'' — элементы из A и j', j'' — элементы из J. Обозначим через H левый идеал, порожденный элементами j' и j''. Очевидно, что $H \leqslant J$; по теореме 1, левый идеал H, порождаемый двумя элементами, является левым аннулятором. Поэтому AH будет подпространством F-пространства A (см. доказательство предложения 4, § 2). Так как оба элемента $a'j'$ и $a''j''$ содержатся в подпространстве AH, то и их сумма и разность $a'j' \pm a''j''$ содержатся в $AH \leqslant AJ$; этим доказано, что множество AJ замкнуто относительно сложения и вычитания. Так как справедливость равенства $AJ = FAJ$ очевидна, то тем самым показано, что AJ является подпространством F-пространства A.

Следствие 2. (а) *Если J — такой левый идеал кольца эндоморфизмов* P, *что подпространство AJ имеет конечный ранг, то $J = Q(AJ)$ является левым аннулятором.*

(б) *Если J — такой правый идеал кольца* P, *что ранг фактор-пространства $A/K(J)$ конечен, то $J = N[K(J)]$ является правым аннулятором.*

Доказательство. Пусть J будет таким левым идеалом, что подпространство AJ имеет конечный ранг; заметим, что AJ является подпространством в силу следствия 1. Так как AJ порождается конечным множеством элементов, то существует такое конечное множество эндоморфизмов $\sigma_1, \ldots, \sigma_n$ из J, что $AJ = \sum_{i=1}^{n} A\sigma_i$. Обозначим через J^* левый идеал, порожденный эндоморфизмами $\sigma_1, \ldots, \sigma_n$. Тогда $AJ = AJ^*$, и, так как J^* порождается конечным числом элементов, то, по теореме 1, J^* является левым аннулятором. Отсюда и из теоремы Б (§ 2) вытекает, что $J^* = Q(AJ^*)$; используя это равенство, легко проверить, что

$$J \leqslant Q(AJ) = Q(AJ^*) = J^* \leqslant J,$$

и, следовательно, $J = Q(AJ)$ является левым аннулятором.

Пусть теперь J — такой правый идеал, что ранг фактор-пространства $A/K(J)$ конечен. Тогда среди всех правых аннуляторов, содержащихся в J, существует такой правый аннулятор J^*, что фактор-пространство $K(J^*)/K(J)$ имеет минимальный ранг [напомним, что из $J^* \leqslant J$ всегда следует $K(J) \leqslant K(J^*)$]. Предположим, что подпространство $K(J^*)$ не совпадает с подпространством $K(J)$. Тогда в $K(J^*)$ существует элемент w, не принадлежащий $K(J)$. В таком случае, по определению подпространства $K(J)$, в J содержится по крайней мере один такой эндоморфизм σ, что $w\sigma \neq 0$. В силу теоремы 1, правый идеал σ^*, порожденный эндоморфизмом σ, будет правым аинулятором; отсюда и из предложения 3 вытекает, что и $J^* + \sigma^*$ является правым аннулятором. Так как w не содержится в $K(J^* + \sigma^*)$, то, очевидно, $K(J^* + \sigma^*) < K(J^*)$, и, следовательно, ранг фактор-пространства $K(J^* + \sigma^*)/K(J)$ будет меньше ранга фактор-пространства $K(J^*)/K(J)$, что противоречит выбору правого аннулятора J^*. Таким образом, $K(J) = K(J^*)$; так как J^* — правый аннулятор, то, по теореме А (§ 2), $J^* = N[K(J^*)]$; отсюда, принимая во внимание, что $K(J)J = 0$, мы получаем

$$J \leqslant N[K(J)] = N[K(J^*)] = J^* \leqslant J,$$

и, следовательно, $J = N[K(J)]$ является правым аннулятором.

Теорема 2. *Следующие свойства линейного многообразия (F, A) эквивалентны:*

(I) *Ранг $r(A)$ конечен.*

(II) *Каждый левый идеал кольца* P *является левым аннулятором.*

(III) *Каждый правый идеал кольца* P *является правым аннулятором.*

Доказательство. Из следствия 2 легко вытекает, что при выполнении свойства (I) выполняются свойства (II) и (III). Если ранг $r(A)$ бесконечен, то рассмотрим совокупность Φ конечнозначных эндоморфизмов σ, т. е. таких σ, для которых $A\sigma$ имеет конечный ранг. Читатель без труда сможет проверить, что Φ является одновременно и левым и правым идеалом кольца P, что $A = A\Phi$ и $0 = K(\Phi)$ и что тождественный эндоморфизм 1 не принадлежит Φ. Следовательно,

$$\Phi < \mathrm{P} = Q(A) = Q(A\Phi) = N(0) = N[K(\Phi)];$$

отсюда и из теорем А и Б (§ 2) вытекает, что Φ не является ни левым, ни правым аннулятором. Этим показано, что свойство (I) следует как из свойства (II), так и из свойства (III).

Замечание 1. Из теоремы 1 следует, что каждый идеал кольца P является суммой аннуляторов, ибо каждый идеал является суммой идеалов, порождаемых конечным множеством элементов (даже суммой главных идеалов). Если ранг $r(A)$ бесконечен, то, согласно теореме 2, не каждый идеал кольца P будет аннулятором. Из этих соображений вытекает, что сумма бесконечного множества аннуляторов может не быть аннулятором; отсюда видно, что в предложении 3 нельзя опустить условие конечности (см. также § 2, замечание 3).

Замечание 2. Если ранг $r(A)$ конечен, то из теоремы 2 и теорем А и Б (§ 2) легко вывести следующие утверждения:

Система подпространств F-пространства A и система правых идеалов кольца эндоморфизмов P двойственны друг другу.

Система подпространств F-пространства A и система левых идеалов кольца эндоморфизмов P проективно эквивалентны.

§ 4. Изоморфизмы кольца эндоморфизмов

Легко видеть, что если ранг линейного многообразия (F, A) равен 1, то кольцо его эндоморфизмов P изоморфно телу F. Поэтому в этом и в следующем параграфе мы будем предполагать, что все рассматриваемые нами линейные многообразия имеют ранги, не меньшие 2; иногда будем предполагать, что ранг линейного многообразия не меньше 3. Читателю следует самому проверить, какие из доказываемых нами теорем остаются справедливыми без этих ограничений.

Рассмотрим два линейных многообразия (F, A) и (G, B) (они могут совпадать или быть различными). Каждое из этих линейных многообразий имеет свое однозначно определенное кольцо эндоморфизмов, соответственно $\mathrm{P}(F, A)$ и $\mathrm{P}(G, B)$; возникает вопрос, в какой мере строение линейного многообразия определяется строением его кольца эндоморфизмов.

Структурная теорема. *Линейные многообразия* (F, A) *и* (G, B) *тогда и только тогда имеют одно и то же строение, когда одинаковое строение имеют их кольца эндоморфизмов* $\mathrm{P}(F, A)$ *и* $\mathrm{P}(G, B)$.

Другими словами, тогда и только тогда существует полулинейное преобразование линейного многообразия (F, A) на линейное многообразие (G, B), когда существует изоморфное отображение кольца $\mathrm{P}(F, A)$ на кольцо $\mathrm{P}(G, B)$ (отображение одного кольца на другое называется изоморфным, если оно взаимно однозначно и сохраняет сложение и умножение). Доказательство этой структурной теоремы будет непосредственно вытекать из наших последующих рассмотрений, в которых мы покажем, что между полулинейными преобразованиями линейного многообразия и изоморфными отображениями его кольца эндоморфизмов существует тесная связь. С этой целью сделаем прежде всего следующее простое замечание.

Пусть σ — полулинейное преобразование F-пространства A на G-пространство B. Тогда σ^{-1} будет полулинейным преобразованием G-пространства B на F-пространство A. Если теперь η есть эндоморфизм линейного многообразия (F, A), то при помощи σ^{-1} отобразим произвольный элемент x G-пространства B на элемент $x^{\sigma^{-1}}$ из A; этот элемент, в свою очередь, при помощи η отобразим на элемент $x^{\sigma^{-1}\eta}$ того же пространства A; полученный в результате элемент при помощи σ отобразим на элемент $(x^{\sigma^{-1}\eta})^{\sigma}$ из B. Произведение

$$\eta^{\sigma} = \sigma^{-1}\eta\sigma$$

наших трех отображений переводит элемент x из B в элемент $(x^{\sigma^{-1}\eta})^{\sigma}$ того же пространства B. Теперь легко проверить, что η^{σ} будет эндоморфизмом G-пространства B и что так определенное соответствие между эндоморфизмом η из $\mathrm{P}(F, A)$ и эндоморфизмом η^{σ} из $\mathrm{P}(G, B)$ является изоморфным отображением кольца $\mathrm{P}(F, A)$ на кольцо $\mathrm{P}(G, B)$. Мы будем говорить, что это изоморфное отображение *индуцируется полулинейным преобразованием* σ. Наше замечание доказывает, в частности, необходимость условия, сформулированного в структурной теореме; достаточность этого условия содержится, очевидно, в следующем утверждении.

Теорема 1. *Каждое изоморфное отображение кольца эндоморфизмов* $\mathrm{P}(F, A)$ *на кольцо эндоморфизмов* $\mathrm{P}(G, B)$ *индуцируется полулинейным преобразованием линейного многообразия* (F, A) *на линейное многообразие* (G, B); *два полулинейных преобразования тогда и только тогда индуцируют одно и то же изоморфное отображение кольца* $\mathrm{P}(F, A)$ *на кольцо* $\mathrm{P}(G, B)$, *когда они индуцируют одно и то же проективное отображение* F-*пространства* A *на* G-*пространство* B.

Доказательству этой основной теоремы мы предпошлем доказательство нескольких лемм.

Лемма 1. *Следующие свойства полулинейного преобразования* τ *F-пространства A на себя эквивалентны:*

(I) $\tau\sigma = \sigma\tau$ *для каждого эндоморфизма* σ *F-пространства A.*

(II) $\tau\sigma = \sigma\tau$ *для каждого идемпотента* σ *из* $\mathrm{P}(F, A)$.

(III) $S^\tau = S$ *для каждого подпространства S F-пространства A.*

(IV) *В теле F существует такое число* $d \neq 0$, *что* $x^\tau = dx$ *для каждого x из A.*

Доказательство. Очевидно, что из свойства (I) следует свойство (II). Пусть для полулинейного преобразования τ выполняется свойство (II). Если S есть подпространство F-пространства A, то существует такой идемпотентный эндоморфизм σ F-пространства A, что $S = A\sigma$. Поэтому, если s — элемент из S, то $s = s\sigma$; отсюда и из свойства (II) вытекает, что элемент

$$s^\tau = (s\sigma)^\tau = (s^\tau)\sigma$$

содержится в $A\sigma = S$. Таким образом, $S^\tau \leqslant S$; теперь, используя полученное включение, нетрудно проверить (это можно сделать различными способами), что для τ справедливо свойство (III). Так как $r(A) > 1$, то можно воспользоваться предложением 3 (гл. III, § 1), в силу которого свойство (IV) является следствием свойства (III). Наконец, если справедливо свойство (IV), то для каждого эндоморфизма σ

$$(x^\tau)\sigma = (dx)\sigma = d(x\sigma) = (x\sigma)^\tau, \text{ откуда } \tau\sigma = \sigma\tau;$$

таким образом, лемма полностью доказана.

Лемма 2. *Если автоморфизм* α *кольца эндоморфизмов* $\mathrm{P}(F, A)$ *оставляет неподвижным каждый идемпотент, то* $\alpha = 1$.

Доказательство. Если σ — элемент кольца эндоморфизмов P, то левый идеал, порожденный σ, обозначим через σ_L, а правый идеал, порожденный σ, обозначим через σ_R. Из теоремы 1 и предложения 1 (§ 3) вытекает, что σ_L и σ_R порождаются идемпотентами. Но автоморфизм α оставляет неподвижным каждый идемпотент; поэтому

$$\sigma_L = (\sigma^\alpha)_L, \quad \sigma_R = (\sigma^\alpha)_R.$$

Из этих равенств непосредственно следует, что

$$K(\sigma) = K(\sigma_R) = K[(\sigma^\alpha)_R] = K(\sigma^\alpha), \quad A\sigma = A\sigma_L = A(\sigma^\alpha)_L = A\sigma^\alpha.$$

Пусть теперь x — произвольный элемент F-пространства A, σ — эндоморфизм этого пространства; предположим, что элементы x и $x\sigma$ линейно независимы. Тогда, поскольку и элементы $x\sigma$, $x - x\sigma$ линейно независимы, легко построить идемпотент $\varkappa$, оставляющий неподвижным элемент $x\sigma$ и отображающий элемент

$x - x\sigma$ на 0. В таком случае

$$0 = x\varkappa - x\sigma\varkappa = x\varkappa - x\sigma, \text{ откуда } x\varkappa = x\sigma.$$

Это показывает, что x содержится в $K(\varkappa - \sigma) = K(\varkappa^\alpha - \sigma^\alpha) = K(\varkappa - \sigma^\alpha)$, т. е. $x\sigma = x\varkappa = x\sigma^\alpha$.

Если элемент x и его образ $x\sigma$ линейно зависимы, но $x \neq 0$, то, поскольку $r(A) > 1$, в A существует элемент y, линейно не зависящий от x. Поэтому существует идемпотент ω, аннулирующий элемент $x - y$ и оставляющий неподвижным элемент y, так что элементы x и $x\omega = y\omega = y$ линейно независимы. Отсюда и из линейной зависимости элементов x и $x\sigma$ следует линейная независимость элементов x и $x\sigma + x\omega = x(\sigma + \omega)$. Применяя теперь к эндоморфизму $\sigma + \omega$ результат предыдущего абзаца и принимая во внимание, что α оставляет неподвижным каждый идемпотент, мы получаем

$$x\sigma + x\omega = x(\sigma + \omega) = x(\sigma + \omega)^\alpha = x\sigma^\alpha + x\omega,$$

откуда $x\sigma = x\sigma^\alpha$. Таким образом, $\sigma = \sigma^\alpha$ для каждого эндоморфизма σ, т. е. $\alpha = 1$.

Заметим, что лемма 2 перестает быть справедливой, когда $r(A) = 1$, ибо в этом случае кольцо P изоморфно телу F.

Лемма 3. *Если σ — полулинейное преобразование линейного многообразия (F, A) на линейное многообразие (G, B), то $\sigma^{-1} N(S)\sigma = N(S^\sigma)$ и $\sigma^{-1} Q(S)\sigma = Q(S^\sigma)$ для каждого подпространства S F-пространства A.*

Доказательство. Легко убедиться в эквивалентности следующих свойств эндоморфизма η линейного многообразия (F, A): η принадлежит $N(S)$; $S\eta = 0$; $0 = (S\eta)^\sigma = S^\sigma(\sigma^{-1}\eta\sigma)$; $\sigma^{-1}\eta\sigma$ принадлежит $N(S^\sigma)$. Отсюда $\sigma^{-1} N(S)\sigma = N(S^\sigma)$.

Аналогично, эквивалентны следующие свойства эндоморфизма η: η принадлежит $Q(S)$; $A\eta \leqslant S$; $B(\sigma^{-1}\eta\sigma) = (A\eta)^\sigma \leqslant S^\sigma$; $\sigma^{-1}\eta\sigma$ принадлежит $Q(S^\sigma)$. Поэтому $\sigma^{-1} Q(S)\sigma = Q(S^\sigma)$.

Лемма 4. *Если σ — изоморфное отображение кольца $\mathrm{P}(F, A)$ на кольцо $\mathrm{P}(G, B)$, то*

(а) *$K[N(S)^\sigma] = BQ(S)^\sigma [= S^{\sigma^*}]$ для каждого подпространства S F-пространства A;*

(б) *σ^* является проективным отображением F-пространства A на G-пространство B.*

Доказательство. Прежде всего заметим, что $L(J)^\sigma = L(J^\sigma)$ для каждого подмножества J кольца $\mathrm{P}(F, A)$. Отсюда и из предложений 1 — 3 (§ 2) вытекает, что

$$K[N(S)^\sigma] = BQ(K[N(S)^\sigma]) = BL[N(S)^\sigma] = B(L[N(S)])^\sigma = BQ(S)^\sigma$$

для каждого подпространства S F-пространства A. Из теоремы Б (§ 2) следует, что отображение подпространства S на подпро-

странство S^{σ^*} определяет проективное отображение F-пространства A на G-пространство B, поскольку σ^* является произведением трех проективных отображений, с помощью которых сначала S отображается на $Q(S)$, затем $Q(S)$ на $Q(S)^\sigma$ [это проективное отображение аннуляторов кольца $\mathrm{P}(F, A)$ на аннуляторы кольца $\mathrm{P}(G, B)$ индуцируется изоморфным отображением σ, при котором образом аннулятора является аннулятор] и, наконец, $Q(S)^\sigma$ на $BQ(S)^\sigma$.

Доказательство теоремы 1. Полулинейные преобразования σ' и σ'' F-пространства A на G-пространство B тогда и только тогда индуцируют одно и то же проективное отображение, когда $S^{\sigma'} = S^{\sigma''}$ для каждого подпространства S F-пространства A. Другими словами, если положить $\sigma = \sigma'\sigma''^{-1}$, то σ' и σ'' тогда и только тогда будут индуцировать одно и то же проективное отображение, когда $S^\sigma = S$ для каждого подпространства S F-пространства A. В силу леммы 1, последнее условие эквивалентно тому, что $\sigma\eta = \eta\sigma$ для каждого эндоморфизма η из $\mathrm{P}(F, A)$. Но это условие, в свою очередь, эквивалентно следующему условию: $\eta^{\sigma'} = \sigma'^{-1}\eta\sigma' = \sigma''^{-1}\sigma^{-1}\eta\sigma\sigma'' = \sigma''^{-1}\eta\sigma'' = \eta^{\sigma''}$ для каждого η из $\mathrm{P}(F, A)$. Таким образом, полулинейные преобразования σ' и σ'' тогда и только тогда индуцируют одно и то же проективное отображение, когда они индуцируют одно и то же изоморфное отображение кольца $\mathrm{P}(F, A)$ на кольцо $\mathrm{P}(G, B)$.

Рассмотрим теперь некоторое изоморфное отображение σ кольца $\mathrm{P}(F, A)$ на кольцо $\mathrm{P}(G, B)$. Из леммы 4 следует, что, отображая подпространство S F-пространства A на подпространство

$$S^{\sigma^*} = K[N(S)^\sigma] = BQ(S)^\sigma,$$

мы получаем проективное отображение F-пространства A на G-пространство B.

[Если бы мы заранее предположили, что ранг F-пространства A не меньше 3, то сейчас можно было бы воспользоваться первой основной теоремой проективной геометрии, с помощью которой мы нашли бы нужное нам полулинейное преобразование; читателю рекомендуется самостоятельно провести детали такого доказательства. Поскольку мы не предполагаем, что $r(A) > 2$, нам придется использовать другой метод построения требуемого полулинейного преобразования.]

Существует прямое разложение $A = P \dotplus H$, где P — точка и H — гиперплоскость. Пусть $P^* = P^{\sigma^*}$ и $H^* = H^{\sigma^*}$. Так как σ^* является проективным отображением, то P^* будет точкой, H^* — гиперплоскостью и $B = P^* \dotplus H^*$. Согласно предложению 5 и замечанию 4 (§ 2), существует полулинейное преобразование τ линейного многообразия (F, A) на линейное многообразие

$[N(H)\bigcap Q(P), N(H)]$, при котором $S^{\tau}=Q(S)\bigcap N(H)$ для каждого подпространства S F-пространства A, и полулинейное преобразование ν линейного многообразия $[N(H^*)\bigcap Q(P^*), N(H^*)]$ на линейное многообразие (G, B), удовлетворяющее условию $T^{\nu^{-1}}=Q(T)\bigcap N(H^*)$ для каждого подпространства T G-пространства B. Нетрудно проверить, что изоморфное отображение σ индуцирует полулинейное преобразование линейного многообразия $[N(H)\bigcap Q(P), N(H)]$ на линейное многообразие $[N(H^*)\bigcap Q(P^*), N(H^*)]$. Следовательно, $\omega=\tau\sigma\nu$ является полулинейным преобразованием F-пространства A на G-пространство B.

Изоморфное отображение σ переводит пересечения идеалов в пересечения их образов и аннуляторы в аннуляторы. Отсюда и из предложения 1 (§ 2) следует, что

$$S^{\tau\sigma}=[Q(S)\bigcap N(H)]^{\sigma}=Q(S)^{\sigma}\bigcap N(H)^{\sigma}=Q[BQ(S)^{\sigma}]\bigcap N(K[N(H)^{\sigma}])=$$
$$=Q[S^{\sigma^*}]\bigcap N[H^{\sigma^*}]=Q(S^{\sigma^*})\bigcap N(H^*)=S^{\sigma^*\nu^{-1}};$$

таким образом, $S^{\sigma^*}=S^{\omega}$ для каждого подпространства S F-пространства A.

Полулинейное преобразование ω индуцирует изоморфное отображение кольца $\mathrm{P}(F, A)$ на кольцо $\mathrm{P}(G, B)$, которое мы обозначим тем же символом ω. По лемме 3,

$$N(S^{\omega})=\omega^{-1}N(S)\omega=N(S)^{\omega} \text{ и } Q(S^{\omega})=\omega^{-1}Q(S)\omega=Q(S)^{\omega};$$

отсюда и из предложения 4 (§ 2) вытекает, что

$$Q(S)^{\sigma}=Q[BQ(S)^{\sigma}]=Q(S^{\sigma^*})=Q(S^{\omega})=Q(S)^{\omega},$$
$$N(S)^{\sigma}=N(K[N(S)^{\sigma}])=N(S^{\sigma^*})=N(S^{\omega})=N(S)^{\omega}.$$

Пусть $\alpha=\sigma\omega^{-1}$. Тогда α будет автоморфизмом кольца $\mathrm{P}(F, A)$, оставляющим инвариантными все $Q(S)$ и $N(S)$. Отсюда и из теорем А и Б (§ 2) следует, что α оставляет инвариантным каждый аннулятор кольца $\mathrm{P}(F, A)$. Если теперь e — произвольный идемпотент из $\mathrm{P}(F, A)$, то, очевидно, и e^{α} будет идемпотентом. Поскольку $\mathrm{P}e=L(1-e)$ и $e\mathrm{P}=R(1-e)$ являются аннуляторами, из наших рассуждений вытекает, что $\mathrm{P}e=\mathrm{P}e^{\alpha}$ и $e\mathrm{P}=e^{\alpha}\mathrm{P}$; отсюда легко вывести, что $e=ee^{\alpha}=e^{\alpha}$. Таким образом, автоморфизм α оставляет неподвижным каждый идемпотент кольца $\mathrm{P}(F, A)$, и, следовательно, по лемме 2, $\alpha=1$, т. е. $\sigma=\omega$. Тем самым показано, что изоморфное отображение σ индуцируется полулинейным преобразованием ω, чем завершается доказательство теоремы 1.

Заметим, что в процессе доказательства теоремы 1 мы доказали справедливость следующего утверждения.

Следствие 1. *Тождественный автоморфизм является единственным автоморфизмом кольца* $\mathrm{P}(F, A)$, *оставляющим инва-*

риантным каждый левый аннулятор $Q(S)$ [*каждый правый аннулятор* $N(S)$][1]).

Теорема 2. *Если* $r(A) \geqslant 3$, *то группа автоморфизмов кольца* $\mathrm{P}(F, A)$ *изоморфна группе автопроективных отображений линейного многообразия* (F, A); *внутренним автоморфизмам кольца* P *при естественном изоморфном отображении первой из этих групп на вторую соответствуют коллинеации* F*-пространства* A.

Доказательство. Если σ — автоморфизм кольца $\mathrm{P}(F, A)$, то положим

$$S^{\sigma^*} = AQ(S)^{\sigma}$$

для каждого подпространства S F-пространства A; из леммы 4 вытекает, что σ^* будет автопроективным отображением F-пространства A для каждого автоморфизма σ кольца P. Легко проверить, что отображение $\sigma \to \sigma^*$ является (естественным) гомоморфным отображением группы автоморфизмов кольца P в группу автопроективных отображений F-пространства A.

Пусть теперь σ — такой автоморфизм кольца P, что $\sigma^* = 1$. В силу теоремы 1, автоморфизм σ индуцируется некоторым полулинейным преобразованием τ F-пространства A. По лемме 3, это, в частности, означает, что

$$Q(S)^{\sigma} = Q(S^{\tau})$$

для каждого подпространства S F-пространства A. Отсюда и из предложения 1 (§ 2) следует, что

$$S = S^{\sigma^*} = AQ(S)^{\sigma} = AQ(S^{\tau}) = S^{\tau}$$

для каждого подпространства S F-пространства A.

Используя теперь лемму 1, мы получаем, что τ индуцирует тождественный автоморфизм кольца P. Таким образом, из $\sigma^* = 1$ следует $\sigma = 1$; тем самым показано, что отображение $\sigma \to \sigma^*$ является изоморфным.

Далее, пусть σ^* — коллинеация. Тогда, как мы показали выше, существует полулинейное преобразование τ, индуцирующее автоморфизм σ и, следовательно, удовлетворяющее условию

$S^{\sigma^*} = S^{\tau}$ для каждого подпространства S F-пространства A.

Так как σ^* — коллинеация, то существует такое линейное преобразование ν, что

$S^{\sigma^*} = S^{\nu}$ для каждого подпространства S F-пространства A;

[1]) В действительности при доказательстве теоремы 1 было доказано более слабое утверждение, а именно, что только тождественный автоморфизм кольца $\mathrm{P}(F, A)$ одновременно оставляет инвариантным и каждый левый аннулятор $Q(S)$ и каждый правый аннулятор $N(S)$. Однако, дополнительно используя теорему B (§ 2), легко показать, что справедливо и более сильное утверждение, сформулированное автором в виде следствия 1. — *Прим. перев.*

отметим, что линейное преобразование ν принадлежит кольцу эндоморфизмов P. Так как ν и τ индуцируют одно и то же автопроективное отображение, то, по теореме 1, они индуцируют один и тот же автоморфизм кольца P. Но полулинейное преобразование τ индуцирует автоморфизм σ; следовательно, и линейное преобразование ν индуцирует автоморфизм σ, а поэтому σ является внутренним автоморфизмом кольца P, индуцированным элементом этого кольца ν. Так как обратное утверждение очевидно, то нами доказано:

(2.1) σ^* *тогда и только тогда будет коллинеацией, когда* σ *является внутренним автоморфизмом кольца* P.

Пусть теперь ω — произвольное автопроективное отображение F-пространства A. Так как $r(A) > 2$, то можно воспользоваться первой основной теоремой проективной геометрии, в силу которой существует полулинейное преобразование τ F-пространства A, индуцирующее ω. Полулинейное преобразование τ индуцирует также такой автоморфизм β кольца P, что $Q(S)^\beta = Q(S^\tau) = Q(S^\omega)$ для каждого подпространства S F-пространства A. Отсюда следует, что

$$S^{\beta^*} = AQ(S)^\beta = AQ(S^\omega) = S^\omega$$

для каждого подпространства S F-пространства A, т. е. $\beta^* = \omega$. Этим наша теорема полностью доказана.

Замечание 1. Предположение, что $r(A) > 2$, было использовано лишь в самом конце доказательства теоремы 2. Поэтому следующее утверждение справедливо при более слабом предположении, что $r(A) \geqslant 2$.

Отображение автоморфизма σ кольца P на автопроективное отображение σ^* F-пространства A является изоморфным отображением группы автоморфизмов кольца P в группу автопроективных отображений F-пространства A; при этом изоморфном отображении группа внутренних автоморфизмов отображается на группу коллинеаций.

Заметим, кроме того, что каждый образ σ^* индуцируется полулинейным преобразованием F-пространства A. Если $r(A) = 2$, то в общем случае могут существовать автопроективные отображения, не индуцированные полулинейными преобразованиями; из сказанного выше следует, что такие автопроективные отображения нельзя представить в виде σ^*.

§ 5. Инверсно изоморфные отображения кольца эндоморфизмов

Для наших последующих рассмотрений оказывается полезным использовать связь между кольцом эндоморфизмов линейного многообразия и кольцом эндоморфизмов пространства, сопряженного

к этому линейному многообразию. Пусть (F, A) — линейное многообразие и (A^*, F) — сопряженное ему пространство (мы используем обозначения, введенные в конце § 2). Поскольку элементы сопряженного пространства A^* умножаются на элементы тела F справа, действие эндоморфизма η сопряженного пространства A^* на элемент x из A^* мы будем обозначать через ηx (так что имеет место равенство $(\eta x)y = \eta(xy)$ для x из A^* и y из F). Произведение эндоморфизмов η и $\varkappa$ сопряженного пространства A^* определим следующим образом:

$$(\eta\varkappa)x = \eta(\varkappa x) \text{ для каждого } x \text{ из } A^*.$$

Определяя обычным способом сложение, мы получим *кольцо эндоморфизмов* $\mathrm{P}(A^*, F)$ сопряженного пространства (A^*, F); очевидно, что для этого кольца остаются справедливыми, с соответствующими изменениями, все утверждения, доказанные нами для колец эндоморфизмов линейных многообразий.

Предложение 1. *Существует, и притом только одно, изоморфное отображение* $\eta \to \eta^*$ *кольца* $\mathrm{P}(F, A)$ *в кольцо* $\mathrm{P}(A^*, F)$, *обладающее следующим свойством*:

$$a(\eta^* b) = (a\eta)b \text{ для } a \text{ из } A,\ b \text{ из } A^* \text{ и } \eta \text{ из } \mathrm{P}(F, A). \qquad (*)$$

Это изоморфное отображение мы будем называть *естественным изоморфным отображением кольца* $\mathrm{P}(F, A)$ *в кольцо* $\mathrm{P}(A^*, F)$.

Доказательство. Пусть η' и η'' являются такими эндоморфизмами сопряженного пространства (A^*, F), что $a(\eta' b) = a(\eta'' b)$ для любых a из A и b из A^*. Тогда эндоморфизм $\eta' - \eta''$ сопряженного пространства A^* обладает свойством $a[(\eta' - \eta'')b] = 0$ для каждого a из A и каждого b из A^*. Но отсюда вытекает, что $0 = (\eta' - \eta'')b$ для каждого b из A^* и, следовательно, $\eta' - \eta'' = 0$, т. е. $\eta' = \eta''$. Этим мы показали, что если изоморфное отображение, обладающее свойством (*), существует, то оно единственно.

Пусть η — эндоморфизм F-пространства A и b — элемент сопряженного пространства A^*; b является линейной формой над A, и отображение элемента a из A на элемент $(a\eta)b$ тела F определяет, очевидно, линейную форму над A. Поскольку эта линейная форма зависит от η и b, мы можем ее обозначить через $\eta^* b$; заметим, что a, b, η и $\eta^* b$ связаны между собой соотношением (*). Нетрудно проверить, что отображение элемента b в элемент $\eta^* b$ определяет эндоморфизм сопряженного пространства A^*, который естественно обозначить через η^*, и что отображение η на η^* является однозначным и сохраняющим сложение и умножение. Если $\eta^* = 0$, то $(a\eta)b = a(\eta^* b) = 0$ для любых a из A и b из A^*; отсюда мы прежде всего получаем, что $a\eta = 0$ для каждого a из A [ибо из $xA^* = 0$, в силу предложения 2 § 3 гл. II, следует $x = 0$], а затем, что $\eta = 0$. Тем самым показано, что отображение

$\eta \to \eta^*$ является требуемым изоморфным отображением кольца $P(F, A)$ в кольцо $P(A^*, F)$.

Предложение 2. *Следующие свойства линейного многообразия* (F, A) *эквивалентны:*

(I) *При естественном изоморфном отображении кольцо* $P(F, A)$ *отображается на кольцо* $P(A^*, F)$.

(II) *Кольца* $P(F, A)$ *и* $P(A^*, F)$ *изоморфны.*

(III) *Ранг* $r(A)$ *конечен.*

Доказательство. Очевидно, что из свойства (I) следует свойство (II). Пусть теперь существует изоморфное отображение σ кольца $P(F, A)$ на кольцо $P(A^*, F)$. По теореме Б (§ 2), отображение подпространства S F-пространства A на левый аннулятор $Q(S)$ из $P(F, A)$ является проективным отображением системы подпространств F-пространства A на совокупность левых аннуляторов кольца $P(F, A)$. Так как σ есть изоморфное отображение, то отображение $Q(S)$ на $Q(S)^\sigma$ будет проективным отображением совокупности левых аннуляторов из $P(F, A)$ на совокупность левых аннуляторов из $P(A^*, F)$. Для того, чтобы можно было применять к сопряженному пространству (A^*, F) и к кольцу его эндоморфизмов $P(A^*, F)$ треугольную теорию Галуа (§ 2), мы должны в формулировках теорем А, Б и В левые аннуляторы заменить правыми, а правые — левыми. Таким образом, из соответствующим образом измененной теоремы А (§ 2) вытекает, что отображение $Q(S)^\sigma$ на $K[Q(S)^\sigma]$ является дуальным отображением совокупности левых аннуляторов кольца $P(A^*, F)$ на совокупность подпространств сопряженного пространства A^*. Следовательно, отображая подпространство S F-пространства A на подпространство $K[Q(S)^\sigma]$ сопряженного пространства A^*, мы получаем дуальное отображение F-пространства A на сопряженное ему пространство A^*. Отсюда и из теоремы существования (гл. IV, § 1) вытекает конечность ранга $r(A)$; тем самым показано, что свойство (III) следует из свойства (II).

Предположим теперь, что выполняется свойство (III). Пусть $\varkappa$ — некоторый эндоморфизм сопряженного пространства A^*. Если a — произвольный фиксированный элемент из A, то отображение элемента b из A^* на число $a(\varkappa b)$ из F определяет линейную форму a' над A^*; это легко проверить прямым подсчетом, принимая во внимание, что каждое $\varkappa b$ является линейной формой над A. Заметим, что a, b, $\varkappa$ и a' связаны между собой соотношением

$$a'b = a(\varkappa b).$$

В силу предположения о конечности ранга $r(A)$ и теоремы 2 (гл. II, § 3), каждая линейная форма над сопряженным пространством A^* индуцируется некоторым элементом F-пространства A. Следовательно, в A существует такой элемент a'', что $a''b = a'b$

для каждого b из A^*. Таким образом, мы можем каждому элементу a из A сопоставить такой элемент a'' того же пространства A, что

$$a''b = a(\varkappa b) \text{ для каждого } b \text{ из } A^*.$$

Легко проверить, что элемент a'' определяется элементом a и предыдущим равенством однозначно (ибо из $ub = vb$, для каждого b из A^*, следует $u = v$). Теперь становится почти очевидным, что отображение элемента a на элемент a'' определяет эндоморфизм η F-пространства A. Этот эндоморфизм η удовлетворяет условию $(a\eta)b = a(\varkappa b)$ для любых a из A и b из A^*; отсюда и из предложения 1 вытекает, что $\eta^* = \varkappa$. Тем самым показано, что при естественном изоморфном отображении кольцо $P(F, A)$ отображается на все кольцо $P(A^*, F)$. Таким образом, из свойства (III) следует свойство (I), и этим предложение 2 полностью доказано.

Прежде чем перейти к основной теме настоящего параграфа, сделаем несколько замечаний общего характера относительно одного способа введения новых понятий. Если T есть определенный класс отображений, каждое из которых, помимо других свойств, обладает свойством сохранения умножения[1]), то отображения, обладающие всеми свойствами T-отображений[2]), за тем исключением, что они отображают произведение элементов на произведение образов этих элементов, взятых в обратном порядке, обычно называют инверсными T-отображениями. Примерами таких отображений являются инверсно изоморфные отображения тел, а также, в более общем случае, инверсно изоморфные отображения колец, которые представляют собой взаимно однозначные отображения σ одного кольца на другое, удовлетворяющие условиям

$$(x+y)^\sigma = x^\sigma + y^\sigma, \quad (xy)^\sigma = y^\sigma x^\sigma.$$

Нам понадобится далее другое понятие подобного рода.

Если (F, A) и (G, B) — линейные многообразия и (A^*, F) — сопряженное к (F, A) пространство, то *инверсно полулинейным преобразованием сопряженного пространства* (A^*, F) *на линейное многообразие* (G, B) мы назовем пару, состоящую из инверсно изоморфного отображения σ' тела F на тело G и изоморфного отображения σ'' аддитивной группы A^* на аддитивную группу B, удовлетворяющих условию

$$(dx)^{\sigma''} = x^{\sigma'} d^{\sigma''} \text{ для } x \text{ из } F \text{ и } d \text{ из } A^*.$$

---

[1]) Предполагается, очевидно, что класс отображений T определен на множестве, в котором операция умножения определена, хотя, вообще говоря, не для всех пар элементов. — *Прим. перев.*

[2]) То есть отображений, принадлежащих классу T.—*Прим. перев.*

Обратное к инверсно полулинейному преобразованию отображение мы также будем считать инверсно полулинейным преобразованием. В дальнейшем всякий раз, когда данное инверсно полулинейное преобразование будет обозначаться через σ, под этим следует подразумевать, что и обе компоненты этого инверсно полулинейного преобразования также обозначаются через σ.

Примером инверсно полулинейного преобразования является тождественное отображение сопряженного пространства на каноническое двойственное пространство (см. гл. IV, § 1). Этот пример показывает, что условие конечности ранга линейного многообразия является достаточным, но не является необходимым для того, чтобы линейное многообразие обладало инверсно полулинейным преобразованием; последним обстоятельством обусловлена необходимость вводимых ниже предположений о конечности рангов рассматриваемых линейных многообразий.

Лемма 1. *Если ранг линейного многообразия* (F, A) *конечен, то для каждого инверсно полулинейного преобразования* σ *сопряженного пространства* (A^*, F) *на линейное многообразие* (G, B) *существует одно и только одно инверсно изоморфное отображение* σ^* *кольца* $\mathrm{P}(F, A)$ *на кольцо* $\mathrm{P}(G, B)$, *обладающее следующими свойствами*:

(а) $(\eta^* d)^\sigma = d^\sigma \eta^{\sigma^*}$ *для* η *из* $\mathrm{P}(F, A)$ *и* d *из* A^* (η^* *является образом эндоморфизма* η *при естественном изоморфном отображении, определенном в предложении* 1).

(б) $N[E(S)^\sigma] = Q(S)^{\sigma^*}$ *и* $Q[E(S)^\sigma] = N(S)^{\sigma^*}$ *для каждого подпространства* S F*-пространства* A.

Мы будем говорить, что инверсно изоморфное отображение σ^* *индуцируется* инверсно полулинейным преобразованием σ.

Доказательство. Если b — элемент G-пространства B, то $b^{\sigma^{-1}}$ будет элементом сопряженного пространства A^*, т. е. линейной формой над A. Так как, в силу предложения 1, при естественном изоморфном отображении каждый эндоморфизм η линейного многообразия (F, A) отображается на эндоморфизм η^* сопряженного пространства (A^*, F), то $\eta^* b^{\sigma^{-1}}$ будет однозначно определенным элементом из A^* для каждого b из B. Поэтому, отображая элемент b на элемент $(\eta^* b^{\sigma^{-1}})^\sigma$, мы получаем однозначное отображение G-пространства B в себя, которое обозначим через η^{σ^*}. Таким образом, отображение η^{σ^*} определяется следующим равенством:

$$b\eta^{\sigma^*} = (\eta^* b^{\sigma^{-1}})^\sigma \text{ для каждого } b \text{ из } B.$$

Отсюда видно, что η^{σ^*} представляет собой результат трех последовательно примененных отображений: сначала применяется отображение σ^{-1}, затем к получающемуся образу применяется отображение η^*, и, наконец, к вновь полученному образу применяется

отображение σ. Таким образом,

$$\eta^{\sigma^*} = \sigma^{-1}\eta^*\sigma.$$

Из предложения 2 и конечности ранга $r(A)$ следует, что при естественном изоморфном отображении кольцо $\mathrm{P}(F, A)$ отображается на все кольцо $\mathrm{P}(A^*, F)$; теперь легко видеть, что отображение эндоморфизма η на эндоморфизм η^{σ^*} определяет инверсно изоморфное отображение кольца $\mathrm{P}(F, A)$ на кольцо $\mathrm{P}(G, B)$, обладающее свойством (а). Справедливость первого из равенств (б), а именно $N[E(S)^\sigma] = Q(S)^{\sigma^*}$, вытекает из эквивалентности следующих утверждений относительно эндоморфизма η F-пространства A:

η принадлежит $Q(S)$; $A\eta \leqslant S$; $A[\eta^* E(S)] = (A\eta)E(S) = 0$;

$\eta^* E(S) = 0$; $0 = [\eta^* E(S)]^\sigma = E(S)^\sigma \eta^{\sigma^*}$; η^{σ^*} принадлежит $N[E(S)^\sigma]$.

Аналогично, равенство $Q[E(S)^\sigma] = N(S)^{\sigma^*}$ непосредственно вытекает из эквивалентности следующих утверждений:

η принадлежит $N(S)$; $0 = S\eta$; $0 = (S\eta)A^* = S(\eta^* A^*)$;

$\eta^* A^* \leqslant E(S)$; $B\eta^{\sigma^*} = (\eta^* A^*)^\sigma \leqslant E(S)^\sigma$; η^{σ^*} принадлежит $Q[E(S)^\sigma]$.

Таким образом, лемма 1 полностью доказана.

Лемма 2. *Если* (F, A) *и* (G, B) *– линейные многообразия и* σ *— инверсно изоморфное отображение кольца* $\mathrm{P}(F, A)$ *на кольцо* $\mathrm{P}(G, B)$, *то*:

(а) $K[Q(S)^\sigma] = BN(S)^\sigma\ [= S^{\sigma^*}]$ *для каждого подпространства* S F*-пространства* A;

(б) σ^* *является дуальным отображением* F*-пространства* A *на* G*-пространство* B.

σ^* называется дуальным отображением, *индуцированным* инверсно изоморфным отображением σ.

Доказательство. Прежде всего заметим, что при инверсно изоморфном отображении σ образом правого аннулятора будет левый аннулятор и наоборот; отсюда, в частности, следует, что $R(J)^\sigma = L(J^\sigma)$ для каждого подмножества J кольца $\mathrm{P}(F, A)$. Принимая это во внимание, мы из предложений 1—3 (§ 2) выводим, что

$$BN(S)^\sigma = B(R[Q(S)])^\sigma = BL[Q(S)^\sigma] = BQ[K(Q(S)^\sigma)] = K[Q(S)^\sigma]$$

для каждого подпространства S F-пространства A. Далее, из теорем А и Б (§ 2) и сделанного выше замечания вытекает, что отображение S на $N(S)$ является дуальным отображением совокупности подпространств F-пространства A на совокупность правых аннуляторов кольца $\mathrm{P}(F, A)$; отображение $N(S)$ на $N(S)^\sigma$

является проективным отображением совокупности правых аннуляторов кольца $P(F, A)$ на совокупность левых аннуляторов кольца $P(G, B)$; отображение $N(S)^{\sigma}$ на $BN(S)^{\sigma}$ является проективным отображением совокупности левых аннуляторов кольца $P(G, B)$ на совокупность подпространств G-пространства B. Таким образом, σ^* является дуальным отображением, как произведение одного дуального и двух проективных отображений.

Теорема существования. *Тогда и только тогда существует инверсно изоморфное отображение кольца эндоморфизмов* $P(F, A)$ *на кольцо эндоморфизмов* $P(G, B)$, *когда ранг* $r(A)$ *конечен и существует инверсно полулинейное преобразование сопряженного пространства* (A^*, F) *на линейное многообразие* (G, B).

Достаточность условий теоремы следует из леммы 1. Если существует инверсно изоморфное отображение кольца $P(F, A)$ на кольцо $P(G, B)$, то, по лемме 2 (б), существует дуальное отображение F-пространства A на G-пространство B; отсюда и из теоремы существования (гл. IV, § 1) следует конечность ранга $r(A)$. Следующая теорема показывает, что существование инверсно изоморфного отображения влечет за собой и существование инверсно полулинейного преобразования.

Теорема 1. *Каждое инверсно изоморфное отображение кольца* $P(F, A)$ *на кольцо* $P(G, B)$ *индуцируется инверсно полулинейным преобразованием сопряженного пространства* (A^*, F) *на линейное многообразие* (G, B).

Здесь мы также предполагаем, что $r(A) > 1$; в соответствии с леммой 1 (а), инверсно изоморфное отображение σ кольца $P(F, A)$ называется индуцированным инверсно полулинейным преобразованием τ сопряженного пространства (A^*, F), если $(\eta^* d)^{\tau} = d^{\tau}\eta^{\sigma}$ для η из $P(F, A)$ и d из A^*, где η^*—образ эндоморфизма η при естественном изоморфном отображении кольца $P(F, A)$ в кольцо $P(A^*, F)$.

Доказательство. Пусть σ—инверсно изоморфное отображение кольца $P(F, A)$ на кольцо $P(G, B)$. По лемме 2, σ индуцирует дуальное отображение σ^*, отображающее подпространство S F-пространства A на подпространство

$$S^{\sigma^*} = BN(S)^{\sigma} = K[Q(S)^{\sigma}]$$

G-пространства B. Из существования дуального отображения следует конечность ранга F-пространства A (теорема существования, гл. IV, § 1). Поэтому в силу предложения 2, при естественном изоморфном отображении $\eta \to \eta^*$ кольцо $P(F, A)$ отображается на все кольцо $P(A^*, F)$.

Существует прямое разложение $A = P \dotplus H$, где P—точка и H—гиперплоскость. Так как σ^* является дуальным отображением, то $P^* = P^{\sigma^*}$ будет гиперплоскостью, $H^* = H^{\sigma^*}$—точкой

и $B = P^* \dotplus H^*$. Поскольку при инверсно изоморфном отображении σ правые аннуляторы отображаются на левые, а левые—на правые, мы из теорем А и Б (§ 2) и равенства, определяющего дуальное отображение σ^*, получаем, что

$$N(S)^{\sigma} = Q(S^{\sigma^*}), \quad Q(S)^{\sigma} = N(S^{\sigma^*})$$

для каждого подпространства S F-пространства A. Применяя теперь дважды предложение 5 (§ 2), мы найдем полулинейное преобразование σ' линейного многообразия (A^*, F) на линейное многообразие $[Q(P), N(H) \cap Q(P)]$, удовлетворяющее условию $E(S)^{\sigma'} = N(S) \cap Q(P)$ для каждого подпространства S F-пространства A, и полулинейное преобразование σ'' линейного многообразия $[N(P^*) \cap Q(H^*), N(P^*)]$ на линейное многообразие (G, B), удовлетворяющее условию $S^{\sigma''^{-1}} = Q(S) \cap N(P^*)$ для каждого подпространства S G-пространства B. В то же время инверсно изоморфное отображение σ индуцирует инверсно полулинейное преобразование линейного многообразия $[Q(P), N(H) \cap Q(P)]$ на линейное многообразие

$$[N(H)^{\sigma} \cap Q(P)^{\sigma}, \; Q(P)^{\sigma}] = [Q(H^*) \cap N(P^*), \; N(P^*)],$$

отображающее $N(S) \cap Q(P)$ на $N(S)^{\sigma} \cap Q(P)^{\sigma} = Q(S^{\sigma^*}) \cap N(P^*)$. Отсюда следует, что произведение $\tau = \sigma' \sigma \sigma''$ является таким инверсно полулинейным преобразованием сопряженного пространства (A^*, F) на линейное многообразие (G, B), что $E(S)^{\tau} = S^{\sigma^*}$ для каждого подпространства S F-пространства A.

Из леммы 1 и конечности ранга $r(A)$ вытекает, что τ индуцирует такое инверсно изоморфное отображение τ^* кольца $P(F, A)$ на кольцо $P(G, B)$, что $Q(S)^{\tau^*} = N[E(S)^{\tau}]$ для каждого подпространства S F-пространства A. Поэтому

$$Q(S)^{\tau^* \sigma^{-1}} = N[E(S)^{\tau}]^{\sigma^{-1}} = N(S^{\sigma^*})^{\sigma^{-1}} = Q(S).$$

Так как σ и τ^*—инверсно изоморфные отображения кольца $P(F, A)$ на кольцо $P(G, B)$, то $\tau^* \sigma^{-1}$ является автоморфизмом кольца $P(F, A)$, оставляющим инвариантным каждый левый аннулятор $Q(S)$. Отсюда и из следствия 1 (§ 4) вытекает, что $\tau^* \sigma^{-1} = 1$, т. е. $\tau^* = \sigma$. Таким образом, нами показано, что инверсно изоморфное отображение σ индуцируется инверсно полулинейным преобразованием τ, чем и завершается доказательство теоремы 1.

Общая теорема существования. *Следующие свойства линейного многообразия (F, A) эквивалентны:*

(I) *Существует инверсно изоморфное отображение кольца эндоморфизмов линейного многообразия (F, A) на кольцо эндоморфизмов некоторого линейного многообразия.*

(II) *Существует дуальное отображение линейного многообразия* (F, A) *на некоторое линейное многообразие.*

(III) *Ранг* $r(A)$ *конечен.*

Доказательство. Если справедливо свойство (I), то, в силу леммы 2, F-пространство A допускает дуальное отображение; таким образом, свойство (II) является следствием свойства (I). Из свойства (II) и теоремы существования (гл. IV, § 1) вытекает конечность ранга $r(A)$, т. е. из свойства (II) следует свойство (III). Предположим теперь, что ранг $r(A)$ конечен. В § 1 гл. IV при построении канонического двойственного пространства мы показали, что тождественное отображение является инверсно полулинейным преобразованием сопряженного пространства (A^*, F) на каноническое двойственное пространство. Поскольку ранг $r(A)$ конечен, можно воспользоваться леммой 1, в силу которой существует инверсно изоморфное отображение кольца эндоморфизмов линейного многообразия (F, A) на кольцо эндоморфизмов канонического двойственного пространства. Таким образом, свойство (I) следует из свойства (III).

Предложение 3. *Пусть* (F, A)*—линейное многообразие, ранг которого конечен,* σ*—инверсно полулинейное преобразование сопряженного пространства* (A^*, F) *на линейное многообразие* (G, B), σ'*—инверсно изоморфное отображение кольца* $\mathrm{P}(F, A)$ *на кольцо* $\mathrm{P}(G, B)$, *индуцированное* σ, *и* σ''*—дуальное отображение* F*-пространства* A *на* G*-пространство* B, *индуцированное* σ'. *Тогда* $S^{\sigma''} = E(S)^{\sigma}$ *для каждого подпространства* S F*-пространства* A.

Доказательство. Положим $S^{\sigma^*} = E(S)^{\sigma}$ для каждого подпространства S F-пространства A. Ввиду конечности ранга $t(A) = n$, мы можем воспользоваться теоремой 3 (гл. II, § 3), из которой следует, что отображение S на $E(S)$ определяет дуальное отображение F-пространства A на сопряженное пространство A^*. Так как σ индуцирует проективное отображение системы подпространств сопряженного пространства A^* на систему подпространств G-пространства B, то σ^* является дуальным отображением F-пространства A на G-пространство B. Отсюда, используя следствие 1 (гл. IV, § 1), мы получаем, что $r(A) = r(B) = n$ и $r(S) + r(S^{\sigma^*}) = n$.

Так как инверсно изоморфное отображение σ' индуцируется инверсно полулинейным преобразованием σ, то, по определению (см. лемму 1),

$$(\eta^* d)^{\sigma} = d^{\sigma} \eta^{\sigma'} \text{ для } \eta \text{ из } \mathrm{P}(F, A) \text{ и } d \text{ из } A^*,$$

где звездочкой обозначено естественное изоморфное отображение кольца $\mathrm{P}(F, A)$ на кольцо $\mathrm{P}(A^*, F)$ (см. предложения 1 и 2), удовлетворяющее условию

$$(a\eta)\, d = a\,(\eta^* d) \text{ для } a \text{ из } A,\ d \text{ из } A^* \text{ и } \eta \text{ из } \mathrm{P}(F, A).$$

Так как дуальное отображение σ'' индуцируется инверсно изоморфным отображением σ', то, по определению (см. лемму 2),

$$S^{\sigma''} = B\,N(S)^{\sigma'}$$

для каждого подпространства S F-пространства A. Используя полученные равенства, мы последовательно найдем, что

$$S[N(S)^*A^*] = [S\,N(S)]\,A^* = 0,$$

$$N(S)^*A^* \leqslant E(S),$$

$$S^{\sigma''} = B\,N(S)^{\sigma'} = A^{*\sigma}\,N(S)^{\sigma'} = [N(S)^*A^*]^{\sigma} \leqslant E(S)^{\sigma} = S^{\sigma^*}.$$

Но так как σ'' является дуальным отображением, то $r(S) + r(S^{\sigma''}) = n$. Отсюда и из равенства, полученного в конце первого абзаца настоящего доказательства, вытекает, что $r(S^{\sigma''}) = r(S^{\sigma^*})$. Воспользовавшись теперь доказанным включением $S^{\sigma''} \leqslant S^{\sigma^*}$ и конечностью всех рассматриваемых здесь рангов, мы получаем, что $S^{\sigma''} = S^{\sigma^*}$. Тем самым предложение 3 полностью доказано.

Теорема единственности. *Если ранг линейного многообразия (F, A) конечен, то следующие свойства инверсно полулинейных преобразований ν и ω сопряженного пространства (A^*, F) на линейное многообразие (G, B) эквивалентны:*

(I) *В G существует такое число $g \neq 0$, что $d^{\nu} = gd^{\omega}$ для каждого элемента d из A^*.*

(II) *ν и ω индуцируют одно и то же инверсно изоморфное отображение кольца $\mathrm{P}(F, A)$ на кольцо $\mathrm{P}(G, B)$.*

(III) *ν и ω индуцируют одно и то же дуальное отображение F-пространства A на G-пространство B.*

Понятие индуцирования инверсно изоморфного отображения инверсно полулинейным преобразованием, о котором идет речь в утверждении (II), нужно понимать в смысле леммы 1; утверждение (III) означает (согласно предложению 3), что $E(S)^{\nu} = E(S)^{\omega}$ для каждого подпространства S F-пространства A.

Доказательство. Если свойство (I) справедливо, то индуцированные инверсно изоморфные отображения ν' и ω' кольца $\mathrm{P}(F, A)$ на кольцо $\mathrm{P}(G, B)$ удовлетворяют условию

$$d^{\nu}\eta^{\nu'} = (\eta^*d)^{\nu} = g(\eta^*d)^{\omega} = g(d^{\omega}\eta^{\omega'}) = (gd^{\omega})\eta^{\omega'} = d^{\nu}\eta^{\omega'}$$

для каждого d из A^* и каждого η из $\mathrm{P}(F, A)$. Но так как d^{ν} пробегает все G-пространство B, то из полученного равенства следует, что $\eta^{\nu'} = \eta^{\omega'}$ для каждого η, т. е. $\nu' = \omega'$. Тем самым показано, что свойство (II) вытекает из свойства (I).

Если ν и ω индуцируют одно и то же инверсно изоморфное отображение σ кольца $\mathrm{P}(F, A)$ на кольцо $\mathrm{P}(G, B)$, то, в силу

предложения 3,

$$E(S)^{\nu} = BN(S)^{\sigma} = E(S)^{\omega}$$

для каждого подпространства S F-пространства A. Отсюда видно, что ν и ω индуцируют одно и то же дуальное отображение F-пространства A на G-пространство B; таким образом, свойство (III) является следствием свойства (II).

Допустим, наконец, что справедливо свойство (III). Тогда $E(U)^{\nu} = E(U)^{\omega}$ для каждого подпространства U F-пространства A. В силу конечности ранга $r(A)$ и теоремы 3 (гл. II, § 3), $T = E[S(T)]$ для каждого подпространства T сопряженного пространства A^*. Отсюда следует, что

$$U^{\nu^{-1}\omega} = E[S(U^{\nu^{-1}})]^{\omega} = E[S(U^{\nu^{-1}})]^{\nu} = U$$

для каждого подпространства U G-пространства B. Но теперь, принимая во внимание, что $\nu^{-1}\omega$ является полулинейным преобразованием G-пространства B, мы воспользуемся предложением 3 (б) (гл. III, § 1), из которого следует существование в G такого числа $g \neq 0$, что $b^{\nu^{-1}\omega} = gb$ для каждого b из B. Полагая $d = b^{\nu^{-1}}$, мы видим, что полученное равенство равносильно свойству (I). Тем самым показано, что из свойства (III) следует свойство (I), чем и завершается доказательство теоремы.

Предложение 4. *Соответствие между изоморфными и инверсно изоморфными отображениями кольца эндоморфизмов, с одной стороны, и индуцированными ими соответственно проективными и дуальными отображениями линейного многообразия, с другой стороны, является мультипликативным, т. е. сохраняет произведение* [1]).

Доказательство. Предположим сначала, что ν есть инверсно изоморфное отображение кольца $P(F, A)$ на кольцо $P(G, B)$, а ω—инверсно изоморфное отображение кольца $P(G, B)$ на кольцо $P(H, C)$. Тогда $\nu\omega$ будет изоморфным отображением кольца $P(F, A)$ на кольцо $P(H, C)$. Каждое из этих отображений индуцирует, согласно лемме 2 и лемме 4 (§ 4), определенное отображение системы подпространств соответствующего линейного многообразия, а именно

$$S^{\nu'} = BN(S)^{\nu} = K[Q(S)^{\nu}]$$

—дуальное отображение F-пространства A на G-пространство B;

$$T^{\omega'} = CN(T)^{\omega} = K[Q(T)^{\omega}]$$

---

[1]) Изоморфное отображение кольца эндоморфизмов индуцирует проективное отображение исходного линейного многообразия в смысле леммы 4 (§ 4).—*Прим. перев.*

—дуальное отображение G-пространства B на H-пространство C;

$$S^{(\nu\omega)'} = CQ(S)^{\nu\omega} = K[N(S)]^{\nu\omega}$$

—проективное отображение F-пространства A на H-пространство C. Используя теперь результаты § 2, мы получаем

$$S^{(\nu\omega)'} = C[Q(S)^{\nu}]^{\omega} = C[N(K[Q(S)^{\nu}])]^{\omega} = C[N(S^{\nu'})]^{\omega} = (S^{\nu'})^{\omega'},$$

откуда следует доказываемое мультипликативное соотношение $(\nu\omega)' = \nu'\omega'$.

Если ν, или ω, или они оба являются изоморфными отображениями, то мультипликативное соотношение проверяется подобным же образом. Детали такой проверки мы оставляем читателю.

Эти мультипликативные соотношения имеют различные применения.

Следствие 1. *Если инверсно изоморфные отображения* ν *и* ω *кольца* $P(F, A)$ *на кольцо* $P(G, B)$ *индуцируют одно и то же дуальное отображение* F*-пространства* A *на* G*-пространство* B, *то* $\nu = \omega$.

Действительно, в этом случае $\nu\omega^{-1}$ будет автоморфизмом кольца $P(F, A)$, индуцирующим тождественное проективное отображение F-пространства A; отсюда и из замечания 1 (§ 4) следует, что $\nu\omega^{-1} = 1$.

РАСШИРЕННЫЕ ГРУППЫ

Совокупность автоморфизмов и инверсных автоморфизмов кольца $P(F, A)$ является группой относительно умножения; эту группу называют *расширенной группой автоморфизмов кольца* $P(F, A)$. Подобным же образом мы определим *расширенную группу автопроективных отображений линейного многообразия* (F, A) как группу всех его автопроективных и автодуальных отображений. Используя следствие 1, легко доказать следующее.

Отображение каждого автоморфизма и каждого инверсного автоморфизма кольца $P(F, A)$ на индуцированное им соответственно автопроективное и автодуальное отображение линейного многообразия (F, A) является изоморфным отображением расширенной группы автоморфизмов кольца $P(F, A)$ в расширенную группу автопроективных отображений линейного многообразия (F, A).

В частности, инволюторные инверсные автоморфизмы кольца $P(F, A)$ индуцируют полярные отображения линейного многообразия (F, A).

Теорема 2. *Если* $r(A) > 2$, *то каждое дуальное отображение линейного многообразия* (F, A) *индуцируется инверсно изоморфным отображением кольца* $P(F, A)$.

Доказательство. Используя лемму 2 (гл. IV, § 1), нетрудно показать, что если $r(A) > 2$, то каждое дуальное отобра-

жение δ линейного многообразия (F, A) на линейное многообразие (G, B) индуцируется инверсно полулинейным преобразованием τ сопряженного пространства (A^*, F) на линейное многообразие (G, B), причем $X^\delta = E(X)^\tau$. Но τ индуцирует также инверсно изоморфное отображение τ' кольца $\mathrm{P}(F, A)$ на кольцо $\mathrm{P}(G, B)$, которое, в свою очередь, индуцирует дуальное отображение, совпадающее, в силу предложения 3, с δ.

Следствие 2. *Если $r(A) > 2$, то из существования автодуальных отображений линейного многообразия (F, A) следует существование инверсных автоморфизмов кольца $\mathrm{P}(F, A)$, и наоборот; аналогично, из существования полярных отображений линейного многообразия (F, A) следует существование инволюторных инверсных автоморфизмов кольца $\mathrm{P}(F, A)$, и наоборот.*

Эти утверждения легко следуют из предыдущих результатов. Детали доказательства мы оставляем читателю.

ПОЛУБИЛИНЕЙНЫЕ ФОРМЫ И ИНВЕРСНЫЕ АВТОМОРФИЗМЫ КОЛЬЦА ЭНДОМОРФИЗМОВ ЛИНЕЙНОГО МНОГООБРАЗИЯ

Пусть ранг линейного многообразия (F, A) конечен и не меньше 3. Тогда, если σ—автодуальное отображение F-пространства A, то, в силу предложения 1 (гл. IV, § 1), σ может быть представлено полубилинейной формой; в то же время σ индуцируется однозначно определенным инверсным автоморфизмом кольца $\mathrm{P}(F, A)$ (теорема 2 и следствие 1). Мы хотим установить связь между полубилинейной формой и инверсным автоморфизмом, определяющими одно и то же автодуальное отображение.

Пусть автодуальное отображение σ представимо полубилинейной формой $f(x, y)$. Если S—подпространство F-пространства A, то S^σ представляет собой совокупность таких элементов x из A, что $f(x, S) = 0$. Рассмотрим, далее, инверсный автоморфизм ν кольца $\mathrm{P}(F, A)$. Инверсный автоморфизм ν тогда и только тогда индуцирует дуальное отображение σ, когда $S^\sigma = K[Q(S)] = AN(S)^\nu$ для каждого подпространства S F-пространства A. Нетрудно проверить, что это условие эквивалентно соотношению

$$f(AN(S)^\nu, S) = 0$$

для каждого подпространства S F-пространства A; при этом нужно воспользоваться тем, что полубилинейная форма f представляет автодуальное отображение.

Из предложения 2 (гл. IV, § 1) следует, что полубилинейная форма f тогда и только тогда представляет автодуальное отображение, когда, отображая элемент a из A на линейную форму a^f, определяемую равенством $xa^f = f(x, a)$ для каждого x из A, мы получаем инверсно полулинейное преобразование F-пространства A на сопряжен-

ное пространство (A^*, F) (второй компонентой этого инверсно полулинейного преобразования будет инверсный автоморфизм тела F, входящий в определение полубилинейной формы f). Теперь, используя результаты настоящего параграфа, нетрудно доказать следующее интересное

Предложение 5. *Инверсный автоморфизм* σ *кольца* $\mathrm{P}(F, A)$ *тогда и только тогда индуцирует автодуальное отображение* F*-пространства* A*, представимое данной полубилинейной формой* f*, когда*

(а) f *представляет некоторое автодуальное отображение и*

(б) $f(x, y\eta) = f(x\eta^{\sigma}, y)$ *для любых* x, y *из* A *и* η *из* $\mathrm{P}(F, A)$.

Детали доказательства мы оставляем читателю.

Замечание. Пусть (F, A) и (G, B)—линейные многообразия одного и того же конечного ранга n, и пусть α—инверсно изоморфное отображение тела F на тело G. Кольцо эндоморфизмов $\mathrm{P}(F, A)$ можно представить как кольцо всех $n \times n$-матриц над телом F; аналогично, кольцо эндоморфизмов $\mathrm{P}(G, B)$ можно представить как кольцо всех $n \times n$-матриц над телом G. Если (a_{ik})—некоторая матрица из $\mathrm{P}(F, A)$, то (a_{ik}) можно отобразить на матрицу $(a_{ik})^{\sigma} = (a_{ki}^{\alpha})$ кольца $\mathrm{P}(G, B)$, сначала транспонируя ее, а затем применяя к каждому ее элементу инверсно изоморфное отображение α. Мы предоставляем читателю самому проверить, что σ является инверсно изоморфным отображением кольца $\mathrm{P}(F, A)$ на кольцо $\mathrm{P}(G, B)$ и что каждое инверсно изоморфное отображение одного из этих колец на другое можно представить в таком виде.

Добавление I

Двусторонние идеалы кольца эндоморфизмов линейного многообразия

Пусть A есть F-пространство конечного или бесконечного ранга и P—кольцо эндоморфизмов этого пространства. Целью настоящего добавления является описание всех двусторонних идеалов кольца P. Напомним, что непустое подмножество J кольца P называется двусторонним идеалом, если $J = J \pm J = J\mathrm{P} = \mathrm{P}J$.

Для произвольного эндоморфизма σ F-пространства A имеет место, согласно формуле (2) (§ 1), равенство $r[A/K(\sigma)] = r[A\sigma]$.

Если $\aleph_\nu$—некоторое (бесконечное) кардинальное число, то обозначим через P_ν совокупность всех таких эндоморфизмов σ F-пространства A, что

$$r[A/K(\sigma)] = r[A\sigma] < \aleph_\nu.$$

(1) P_ν *является двусторонним идеалом кольца* P.

Доказательство. Если эндоморфизмы σ' и σ'' оба принадлежат P_ν, то, поскольку $A(\sigma' \pm \sigma'') \leqslant A\sigma' + A\sigma''$ и $r(A\sigma' + A\sigma'') \leqslant$

$\leqslant r(A\sigma') + r(A\sigma'') < 2\aleph_\nu = \aleph_\nu$, в P_ν содержатся также и эндоморфизмы $\sigma' \pm \sigma''$. Если $\sigma \in \mathrm{P}_\nu$ и $\eta \in \mathrm{P}$, то $A\eta\sigma \leqslant A\sigma$ и, следовательно, $r(A\eta\sigma) \leqslant r(A\sigma) < \aleph_\nu$, так что $\eta\sigma$ содержится в P_ν. Так как $K(\sigma) \leqslant K(\sigma\eta)$, то $r[A/K(\sigma\eta)] \leqslant r[A/K(\sigma)] < \aleph_\nu$; таким образом, и $\sigma\eta$ принадлежит P_ν. Этим показано, что каждое P_ν является двусторонним идеалом кольца P.

Заметим, что P_0 состоит из всех эндоморфизмов σ, удовлетворяющих условию: ранг $r[A/K(\sigma)] = r[A\sigma]$ конечен; отсюда непосредственно следует, что

(2) $\mathrm{P} = \mathrm{P}_0$ *тогда и только тогда, когда F-пространство A имеет конечный ранг.*

Легко заметить, что

(3) $0 < \mathrm{P}_0 \leqslant \ldots \leqslant \mathrm{P}_\nu \leqslant \ldots$.

Докажем теперь:

(4) *Если* $\aleph_\nu \leqslant r(A)$, *то* $\mathrm{P}_\nu < \mathrm{P}_{\nu+1}$; *если* $r(A) < \aleph_\nu$, *то* $\mathrm{P}_\nu = \mathrm{P}$.

Доказательство. Если $\aleph_\nu \leqslant r(A)$, то в A существует подпространство U, имеющее ранг $\aleph_\nu$. Существует идемпотентный эндоморфизм σ, отображающий A на U. Эндоморфизм σ содержится в $\mathrm{P}_{\nu+1}$ и не содержится в P_ν. Если же $r(A) < \aleph_\nu$, то тождественный эндоморфизм содержится в двустороннем идеале P_ν и, следовательно, P_ν совпадает со всем кольцом P.

(5) *Если* J *— произвольный двусторонний идеал кольца* P *и* σ *— элемент из* J, *то* J *содержит каждый эндоморфизм* η, *удовлетворяющий условию* $r(A\eta) \leqslant r(A\sigma)$.

Доказательство. Так как $r(A\eta) \leqslant r(A\sigma)$, то существует взаимно однозначное отображение некоторой части базиса подпространства $A\sigma$ на базис подпространства $A\eta$; используя это, легко построить эндоморфизм σ'' F-пространства A, отображающий $A\sigma$ на $A\eta$. Эндоморфизм $\sigma\sigma''$ содержится в J и $A\sigma\sigma'' = A\eta$. В силу леммы 1 (§ 3), существует такой эндоморфизм σ', что $\sigma'(\sigma\sigma'')$ является идемпотентом, удовлетворяющим условию $A\sigma'\sigma\sigma'' = A\sigma\sigma'' = A\eta$. Очевидно, что $\sigma'\sigma\sigma''$ содержится в двустороннем идеале J и, следовательно, $\eta(\sigma'\sigma\sigma'')$ принадлежит J. Но так как $\sigma'\sigma\sigma''$ является идемпотентом, то он оставляет неподвижным каждый элемент подпространства $A\sigma'\sigma\sigma'' = A\eta$; отсюда следует, что $\eta = \eta\sigma'\sigma\sigma''$, и этим доказано, что η содержится в J.

(6) *Каждый отличный от* 0 *двусторонний идеал* J *кольца* P *совпадает с одним из идеалов* P_ν.

Доказательство. Пусть J — произвольный отличный от 0 двусторонний идеал кольца P. Если $J = \mathrm{P}$, то, в силу утверждения (4), $J = \mathrm{P}_\nu$ для некоторого ν. Предположим теперь, что $0 < J < \mathrm{P}$. Тогда, используя утверждение (5) и условие $J \neq 0$, легко показать, что $\mathrm{P}_0 \leqslant J$. Поскольку $J \neq \mathrm{P}$, существует такое трансфинитное число ν, что J содержит не все эндоморфизмы σ, удовлетворяющие условию $r(A\sigma) \leqslant \aleph_\nu$ [например, трансфинитное число ν, при котором $r(A) < \aleph_\nu$]. Среди таких трансфинитных

чисел существует наименьшее, которое мы обозначим через τ. Таким образом, J содержит не все эндоморфизмы σ, удовлетворяющие условию $r(A\sigma) \leqslant \aleph_\tau$, и в то же время содержит каждый эндоморфизм σ, удовлетворяющий условию $r(A\sigma) < \aleph_\tau$. Применяя теперь утверждение (5), мы убеждаемся, что $J = P_\tau$; тем самым утверждение (6) полностью доказано.

Содержание настоящего добавления следует рассматривать как первый шаг в решении задачи охарактеризовать кольца эндоморфизмов внутренними свойствами. Другие результаты в этом направлении читатель может найти в таких книгах по теории колец, как Алберт [1], Артин, Несбитт, Тролл [1], Джекобсон [2]; в работе Бэра [3] аналогичная проблема решается для более общего случая; кроме того, см. следующие работы по теории простых колец: Артин [2], Артин и Уэйплс [1], Джекобсон [1], Джонсон [1][1]).

[1]) В работе Вольфсона [1] указаны необходимые и достаточные условия для того, чтобы кольцо было изоморфно полному кольцу эндоморфизмов некоторого F-пространства A. Таким образом, проблема, поставленная в последнем абзаце настоящего добавления, уже решена.—*Прим. перев.*

ГЛАВА VI

ГРУППЫ ЛИНЕЙНОГО МНОГООБРАЗИЯ

В § 2 гл. III мы изучали некоторые группы, которые можно связать с данным линейным многообразием (F, A). Напомним группу $\Lambda(F, A)$ его полулинейных преобразований, группу $\mathrm{T}(F, A)$ линейных преобразований, группу автопроективных отображений, группу коллинеаций, а также расширенную группу автопроективных отображений, о которой мы упомянули в § 5 гл. V. При рассмотрении любой из этих групп можно поставить вопрос, в какой мере ее строение определяет строение исходного линейного многообразия.

В настоящей главе мы с этой точки зрения исследуем только группы T и Λ; при этом будем предполагать, что характеристика исходного линейного многообразия отлична от 2 и что ранг этого линейного многообразия не меньше 3. При таких предположениях мы докажем эквивалентность следующих свойств линейных многообразий (F, A) и (G, B):

(I) $\mathrm{T}(F, A) \sim \mathrm{T}(G, B)$;

(II) $\Lambda(F, A) \sim \Lambda(G, B)$;

(III) Линейные многообразия (F, A) и (G, B) либо проективно эквивалентны, либо двойственны друг другу.

Доказательство эквивалентности указанных утверждений будет следовать из теорем, в которых исчерпывающим образом описываются все изоморфные отображения, если они существуют, группы $\mathrm{T}(F, A)$ на группу $\mathrm{T}(G, B)$ и группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$. Эти теоремы содержатся соответственно в §§ 5 и 7 настоящей главы.

В свою очередь результаты §§ 5 и 7 опираются на результаты §§ 1—4, цель которых — истолковать «аддитивные» свойства линейных преобразований в терминах «мультипликативных» свойств; здесь под аддитивными свойствами подразумеваются те свойства линейного преобразования, которые характеризуют его как определенное преобразование исходного линейного многообразия; мультипликативными же свойствами мы называем свойства линейного преобразования как элемента группы линейных преобразований, рассматриваемой в качестве абстрактной группы. Результаты, относящиеся к группе полулинейных преобразований Λ, мы выведем из результатов, относящихся к группе линейных преобразо-

ваний T. Для этого в § 6 будет показано, что T является характеристической подгруппой группы Λ. Истолкование аддитивных свойств на языке мультипликативных делает возможным восстановление исходного линейного многообразия по его группе.

Исследование группы коллинеаций в рамках теории групп перестановок проведено в работе Титса [1]. С изучением изоморфных отображений и (особенно) автоморфизмов групп проективной геометрии читатель может познакомиться по классической работе Шрейера и Ван-дер-Вардена [1] и по более современным работам Дьёдонне [1, 2], Рикарта [1, 3], Хуа Ло-гэна [1, 3] и Макки [1].

Замечание относительно обозначений. В первой части настоящей главы мы будем изучать группу линейных преобразований, причем эта группа будет рассматриваться как группа единиц кольца эндоморфизмов P. Поэтому в этой части нашего исследования оказывается удобным обозначать действие линейного преобразования на элемент исходного линейного многообразия в виде умножения этого элемента на линейное преобразование справа. В то же время в последних двух параграфах настоящей главы будет рассматриваться группа полулинейных преобразований, и здесь более удобно записывать образ элемента при полулинейном преобразовании в виде степени этого элемента. Таким образом, мы будем пользоваться мультипликативной записью в первых параграфах и показательной записью в последних двух параграфах.

§ 1. Центр полной линейной группы [1])

Если (F, A) - линейное многообразие, то через T или $T(F, A)$ обозначим группу всех его линейных преобразований. Подмножество Z или $Z(F, A)$ группы T, состоящее из всех линейных преобразований, перестановочных с каждым линейным преобразованием из T, называется *центром* группы T. Нам необходимо охарактеризовать эту абелеву характеристическую подгруппу группы T.

Предложение 1. *Если* $r(A) > 1$, *то следующие свойства линейного преобразования* σ *эквивалентны.*

(I) σ *содержится в центре* Z *группы* T.

(II) σ *оставляет инвариантным каждое подпространство* F*-пространства* A.

(III) *В центре тела* F *существует такое число* $z \neq 0$, *что* $x\sigma = zx$ *для каждого* x *из* A.

Доказательство. Предположим сначала, что справедливо свойство (I). Если бы x и $x\sigma$ были линейно независимыми элемен-

[1]) То есть группы всех линейных преобразований линейного многообразия на себя.—*Прим. перев.*

тами F-пространства A, то оба они были бы отличны от 0; поэтому в A существовало бы такое подпространство T, что $A = Fx \dotplus Fx\sigma \dotplus T$ (принцип дополнения). Очевидно, что существует, и притом только одно, такое линейное преобразование τ F-пространства A, при котором $y\tau = y$ для каждого y из $Fx + T$ и $x\sigma\tau = x + x\sigma$. Но так как $x\tau\sigma = x\sigma$, то линейные преобразования σ и τ не перестановочны, что противоречит свойству (I). Тем самым нами показано, что для каждого x из A элементы x и $x\sigma$ являются линейно зависимыми; но это означает, что $Fx = (Fx)\sigma$ для каждого x из A. Таким образом, из свойства (I) следует свойство (II).

Пусть теперь выполняется свойство (II). Тогда, в силу предложения 3 (гл. III, § 1), в теле F существует такое число $z \neq 0$, что $x\sigma = zx$ для каждого x из A. Если теперь g — произвольное число из F, то

$$(gz)x = g(zx) = g(x\sigma) = (gx)\sigma = z(gx) = (zg)x$$

для каждого x из A; отсюда вытекает, что $gz = zg$ для каждого g из F, поскольку всегда можно выбрать x отличным от 0. Таким образом, z содержится в центре тела F. Тем самым показано, что свойство (III) следует из свойства (II). Наконец, очевидно, что при выполнении свойства (III) выполняется и свойство (I).

Замечание 1. Если $r(A) = 1$, то остается справедливым утверждение об эквивалентности свойств (I) и (III). В то же время, поскольку в этом случае каждое линейное преобразование обладает свойством (II), то читатель может легко убедиться в неэквивалентности свойств (II) и (I), если тело F не коммутативно.

Предложение 2. *Центр* Z *группы* T *изоморфен мультипликативной группе центра тела* F.

Это утверждение непосредственно следует из предложения 1 и замечания 1.

Замечание 2. В силу предложения 2, строение мультипликативной группы центра тела F полностью определяется строением линейной группы T. Существует, однако, много неизоморфных полей, мультипликативные группы которых изоморфны. Например, нетрудно проверить, что мультипликативные группы алгебраически замкнутых полей F' и F'' изоморфны тогда и только тогда, когда поля F' и F'' состоят из одного и того же числа элементов и имеют одну и ту же характеристику. В то же время остается открытым вопрос, какие же инварианты тела F, подобно его характеристике, определяются строением мультипликативной группы центра тела F.

Замечание 3. Ввиду установленной тесной связи между центром тела F и центром группы T, можно, не опасаясь недоразумений,

и это мы будем в дальнейшем делать, обозначать отображение $x \to zx$ (элемент x пробегает все A, а z — фиксированный элемент из центра тела F) буквой z.

§ 2. Первый и второй централизаторы инволюции

Если σ — произвольное отображение линейного многообразия (F, A) в себя, то совокупность элементов x из A, удовлетворяющих условию $x\sigma = x$, обозначим через $J^+(\sigma)$, а совокупность элементов x из A, удовлетворяющих условию $x\sigma = -x$, через $J^-(\sigma)$. Если σ является линейным преобразованием или — более общий случай — эндоморфизмом, то $J^+(\sigma)$ и $J^-(\sigma)$ будут подпространствами линейного многообразия (F, A). Если характеристика тела F равна 2, то подпространства $J^+(\sigma)$ и $J^-(\sigma)$ совпадают; если же характеристика тела F отлична от 2, то единственным общим элементом этих подпространств будет 0. Именно в связи с последним обстоятельством мы будем, начиная с этого параграфа и до конца настоящей главы, всюду предполагать, что *характеристика тела F отлична от 2*. В то же время читателю следует проверять, какие из доказываемых нами утверждений остаются справедливыми без указанного предположения.

Если Θ есть некоторое подмножество линейной группы $\mathrm{T}(F, A)$ рассматриваемого линейного многообразия, то через $\mathrm{Z}(\Theta)$ мы обозначим совокупность всех линейных преобразований ζ, перестановочных с каждым σ из Θ. Очевидно, что $\mathrm{Z}(\Theta)$ является подгруппой группы T; эта подгруппа называется *централизатором подмножества Θ (в группе* T). Иногда мы будем образовывать централизатор от централизатора; для этого *второго централизатора* множества Θ будет использоваться обозначение $\mathrm{Z}_2(\Theta) = \mathrm{Z}[\mathrm{Z}(\Theta)]$.

Рассмотрим теперь произвольную инволюцию σ F-пространства A, т. е. линейное преобразование, удовлетворяющее условию $\sigma^2 = 1$. Используя лемму 1 (гл. IV, § 5), легко проверить, что линейное преобразование σ тогда и только тогда является инволюцией, когда

$$A = J^+(\sigma) \dotplus J^-(\sigma).$$

Централизатор инволюции полностью описывает следующее

Предложение 1. *Следующие свойства инволюции σ и линейного преобразования τ эквивалентны:*

(I) $\sigma\tau = \tau\sigma$.

(II) $J^+(\sigma)\tau \leqslant J^+(\sigma)$ *и* $J^-(\sigma)\tau \leqslant J^-(\sigma)$.

(III) $J^+(\sigma)\tau = J^+(\sigma)$ *и* $J^-(\sigma)\tau = J^-(\sigma)$.

Доказательство. Предположим сначала, что выполняется свойство (I). Тогда, если $x = x\sigma$, то $x\tau = x\sigma\tau = x\tau\sigma$. Тем самым доказано, что $J^+(\sigma)\tau \leqslant J^+(\sigma)$; подобным же образом можно убедиться, что $J^-(\sigma)\tau \leqslant J^-(\sigma)$. Таким образом, из свойства (I) следует

свойство (II). Если линейное преобразование τ удовлетворяет условию (I), то то же самое справедливо и для τ^{-1}. Отсюда, как показано выше, следует, что τ и τ^{-1} оба удовлетворяют условию (II). Используя это замечание, мы получаем, что

$$J^+(\sigma) = J^+(\sigma)\tau^{-1}\tau \leqslant J^+(\sigma)\tau \leqslant J^+(\sigma), \text{ откуда } J^+(\sigma)\tau = J^+(\sigma).$$

Из тех же соображений видно, что $J^-(\sigma)\tau = J^-(\sigma)$; тем самым показано, что и свойство (III) следует из свойства (I).

Очевидно, что из свойства (III) следует свойство (II). Пусть, наконец, выполняется свойство (II). Тогда, если x — элемент из $J^+(\sigma)$, то в $J^+(\sigma)$ содержится и элемент $x\tau$; поэтому

$$x\sigma\tau = x\tau = x\tau\sigma;$$

если же элемент x принадлежит $J^-(\sigma)$, то подобным же образом доказывается, что

$$x\sigma\tau = -x\tau = x\tau\sigma.$$

Поскольку $A = J^+(\sigma) \dot{+} J^-(\sigma)$, из двух полученных равенств следует, что $\sigma\tau = \tau\sigma$.

Следствие 1. *Если σ — инволюция, то ее централизатор $\mathrm{Z}(\sigma)$ изоморфен прямому произведению групп $\mathrm{T}(F, J^+(\sigma))$ и $\mathrm{T}(F, J^-(\sigma))$.*

Точный смысл термина «прямое произведение групп» станет ясен в процессе доказательства.

Доказательство. Обозначим через $\mathrm{Z}^+(\sigma)$ совокупность линейных преобразований ζ, принадлежащих $\mathrm{Z}(\sigma)$ и удовлетворяющих условию $x\zeta = x$ для каждого x из $J^-(\sigma)$; через $\mathrm{Z}^-(\sigma)$ обозначим совокупность линейных преобразований ζ, также принадлежащих $\mathrm{Z}(\sigma)$, но удовлетворяющих условию $x\zeta \neq x$ для каждого x из $J^+(\sigma)$. Очевидно, что $\mathrm{Z}^+(\sigma)$ и $\mathrm{Z}^-(\sigma)$ являются подгруппами группы $\mathrm{Z}(\sigma)$ и что

$$\mathrm{Z}^+(\sigma) \cap \mathrm{Z}^-(\sigma) = 1. \tag{1}$$

Докажем теперь следующие утверждения.

(2) Каждый элемент подгруппы $\mathrm{Z}^+(\sigma)$ перестановочен с каждым элементом подгруппы $\mathrm{Z}^-(\sigma)$.

Действительно, пусть линейные преобразования σ' и σ'' содержатся соответственно в $\mathrm{Z}^+(\sigma)$ и $\mathrm{Z}^-(\sigma)$. Тогда, если x — элемент из $J^+(\sigma)$, то, в силу предложения 1, элемент $x\sigma'$ также принадлежит $J^+(\sigma)$ и, следовательно, $x\sigma'\sigma'' = x\sigma' = x\sigma''\sigma'$; подобным же образом доказывается, что $x\sigma'\sigma'' = x\sigma''\sigma'$ для каждого x из $J^-(\sigma)$. Отсюда, принимая во внимание, что $A = J^+(\sigma) \dot{+} J^-(\sigma)$, мы получаем равенство $\sigma'\sigma'' = \sigma''\sigma'$.

$$\mathrm{Z}(\sigma) = \mathrm{Z}^+(\sigma)\,\mathrm{Z}^-(\sigma). \tag{3}$$

В самом деле, если линейное преобразование ζ принадлежит $Z(\sigma)$, то, согласно предложению 1, $J^+(\sigma)\zeta = J^+(\sigma)$. Отсюда следует, что ζ индуцирует на $J^+(\sigma)$ линейное преобразование. Так как $A = J^+(\sigma) + J^-(\sigma)$, то существует, и притом только одно, такое линейное преобразование ζ' F-пространства A, что

$$x\zeta' = \begin{cases} x\zeta & \text{для } x \text{ из } J^+(\sigma), \\ x & \text{для } x \text{ из } J^-(\sigma). \end{cases}$$

Из предложения 1 непосредственно следует, что ζ' принадлежит $Z^+(\sigma)$. Используя теперь определение линейного преобразования ζ', мы получаем, что линейное преобразование $\zeta'' = \zeta\zeta'^{-1}$ принадлежит $Z^-(\sigma)$. Таким образом, $\zeta = \zeta''\zeta' = \zeta'\zeta''$ [в силу (2)] содержится в $Z^+(\sigma)Z^-(\sigma)$, чем и завершается доказательство утверждения (3).

Справедливость утверждений (1), (2) и (3) как раз и означает, что

$$Z(\sigma) = Z^+(\sigma) \times Z^-(\sigma) \tag{4}$$

(где $\times$ обозначает прямое произведение).

Если ζ принадлежит $Z^+(\sigma)$, то, в силу предложения 1, ζ индуцирует на $J^+(\sigma)$ определенное линейное преобразование ζ^*. Нетрудно проверить, что отображение ζ в ζ^* задает изоморфное отображение подгруппы $Z^+(\sigma)$ на группу $T(F, J^+(\sigma))$; точно так же очевидна изоморфность подгруппы $Z^-(\sigma)$ и группы $T(F, J^-(\sigma))$. Опираясь на это замечание и утверждение (4), легко убеждаемся в справедливости следствия 1.

Мы подготовлены теперь к тому, чтобы дать полное описание второго централизатора инволюции.

Предложение 2. *Линейное преобразование τ тогда и только тогда принадлежит второму централизатору $Z_2(\sigma)$ инволюции σ, когда в центре тела F существуют такие числа h, k (отличные от 0), что $x\tau = hx$ для каждого x из $J^+(\sigma)$ и $x\tau = kx$ для каждого x из $J^-(\sigma)$.*

Доказательство. Предположим сначала, что линейное преобразование τ удовлетворяет условию нашего предложения и что ζ произвольное линейное преобразование, принадлежащее $Z(\sigma)$. Тогда, если x – элемент из $J^+(\sigma)$, то, в силу предложения 1, в $J^+(\sigma)$ содержится также элемент $x\zeta$; отсюда и из нашего предположения вытекает, что $x\tau\zeta = hx\zeta = x\zeta\tau$. Если же x принадлежит $J^-(\sigma)$, то аналогично доказывается, что $x\tau\zeta = kx\zeta = x\zeta\tau$. Так как $A = J^+(\sigma) + J^-(\sigma)$, то из полученных равенств следует, что $\tau\zeta = \zeta\tau$; тем самым доказана достаточность нашего условия.

Обратно, пусть τ принадлежит $Z_2(\sigma)$. Так как инволюция σ перестановочна сама с собой, то σ содержится в $Z(\sigma)$. Таким

образом, τ должно быть перестановочно с σ, и, следовательно, в силу предложения 1, $J^+(\sigma)\tau = J^+(\sigma)$ и $J^-(\sigma)\tau = J^-(\sigma)$. При доказательстве следствия 1 было показано, что каждое линейное преобразование F-пространства $J^+(\sigma)$ индуцируется линейным преобразованием F-пространства A, содержащимся в $Z(\sigma)$. Поскольку τ перестановочно с каждым линейным преобразованием из $Z(\sigma)$, τ индуцирует на $J^+(\sigma)$ такое линейное преобразование, которое перестановочно с любым линейным преобразованием F-пространства $J^+(\sigma)$ [т. е. содержится в центре группы $T(F, J^+(\sigma))$]. Теперь воспользуемся предложением 1 (§ 1) [и замечанием 1 (§ 1) в случае, если $r[J^+(\sigma)] = 1$], из которого следует существование в центре тела F такого числа $h \neq 0$, что $x\tau = hx$ для каждого x из $J^+(\sigma)$. Подобным же образом доказывается существование в центре тела F такого числа $k \neq 0$, что $x\tau = kx$ для каждого x из $J^-(\sigma)$, чем и завершается доказательство предложения.

Замечание 1. Если σ есть инволюция F-пространства A, то совокупность линейных преобразований из $Z_2(\sigma)$, оставляющих неподвижным каждый элемент подпространства $J^-(\sigma)$, обозначим через $Z_2^+(\sigma)$. Из только что доказанного предложения 2 и предложения 2 § 1 следует, что центр Z группы $T(F, A)$ и подгруппа $Z_2^+(\sigma)$ изоморфны одной и той же мультипликативной группе отличных от 0 чисел из центра тела F и что

$$Z_2(\sigma) = Z \times Z_2^+(\sigma).$$

Следствие 2. *Если σ — инволюция, τ — линейное преобразование, содержащееся в $Z_2(\sigma)$, и x — элемент F-пространства A, то*

$$r\left(\sum_{i=0}^{\infty} Fx\tau^i\right) \leqslant 2 \text{ и } \left(\sum_{i=0}^{\infty} Fx\tau^i\right)\tau = \sum_{i=0}^{\infty} Fx\tau^i.$$

Доказательство. В силу предложения 2, в центре тела F существуют такие отличные от 0 числа h и k, что

$$y\tau = \begin{cases} hy & \text{для } y \text{ из } J^+(\sigma), \\ ky & \text{для } y \text{ из } J^-(\sigma). \end{cases} \qquad (*)$$

Пусть теперь x — произвольный элемент F-пространства A, и пусть $X = \sum_{i=0}^{\infty} Fx\tau^i$. Так как σ является инволюцией, то $A = J^+(\sigma) + J^-(\sigma)$, и, следовательно, существуют такие однозначно определенные элементы x' и x'', содержащиеся соответственно в $J^+(\sigma)$ и $J^-(\sigma)$, что $x = x' + x''$. Теперь, используя формулу (*), мы найдем, что $x\tau^i = h^i x' + k^i x''$. Отсюда видно, что $X \leqslant Fx' + Fx''$ и, следовательно, $r(X) \leqslant 2$. Из определения подпространства X вытекает, что $X\tau \leqslant X$; в то же время, поскольку τ является линейным преобразованием, подпространства X и $X\tau$ имеют один и тот же

конечный ранг. Пользуясь теперь формулой для ранга (а) (гл. II, § 2), мы получаем, что $X = X\tau$, и этим следствие 2 полностью доказано.

Следующее предложение, которым мы будем в дальнейшем пользоваться, является до некоторой степени обратным предложению 1.

Предложение 3. *Если σ есть инволюция и S — подпространство линейного многообразия (F, A), то тогда и только тогда $S = S\tau$ для каждой инволюции τ из $Z(\sigma)$, когда S есть либо 0, либо $J^+(\sigma)$, либо $J^-(\sigma)$, либо A.*

Доказательство. Достаточность этих условий непосредственно следует из предложения 1. Пусть теперь $S = S\tau$ для каждой инволюции τ, принадлежащей централизатору $Z(\sigma)$. Положим $T = S \cap J^+(\sigma)$. В силу предложения 1,

$$J^+(\sigma)\tau = J^+(\sigma)$$

для каждой инволюции τ из $Z(\sigma)$; отсюда следует, что

$T\tau = T$ для каждой инволюции τ, принадлежащей $Z(\sigma)$. (*)

Допустим теперь, вопреки утверждению, что $0 < T < J^+(\sigma)$. Тогда T содержит элемент $v \neq 0$, а $J^+(\sigma)$ содержит элемент w, не принадлежащий T. В таком случае существуют такие подпространства V и W, что $T = Fv + V$ и $J^+(\sigma) = T + Fw + W$. Следовательно,

$$J^+(\sigma) = Fv + V + Fw + W = F(v + w) + V + Fw + W.$$

Поэтому существует, и притом только одна, такая инволюция τ, при которой $(v + w)\tau = -v - w$ и $x\tau = x$ для каждого x из $V + Fw + W + J^-(\sigma)$. Из предложения 1 следует, что $\sigma\tau = \tau\sigma$. Но

$$v\tau = v\tau + w\tau - w = -v - 2w.$$

Так как w содержится в $J^+(\sigma)$ и не содержится в $T = S \cap J^+(\sigma)$, а v принадлежит T, то элементы w и $-v - 2w$ не принадлежат S. Таким образом, $S\tau$ не является частью подпространства S, что противоречит нашему предположению. Тем самым показано, что $S \cap J^+(\sigma)$ может быть либо 0, либо $J^+(\sigma)$; подобным же образом можно убедиться, что $S \cap J^-(\sigma)$ совпадает либо с 0, либо с $J^-(\sigma)$. Но отсюда следует, что S равно либо 0, либо $J^+(\sigma)$, либо $J^-(\sigma)$, либо A; таким образом, предложение 3 доказано.

§ 3. Линейные преобразования класса 2

Линейное преобразование σ называется линейным преобразованием *конечного класса*, если $(\sigma - 1)^i = 0$ для некоторого целого положительного числа i; наименьшее натуральное число i,

удовлетворяющее этому условию, называется *классом линейного преобразования* σ. Таким образом, линейное преобразование σ тогда и только тогда является *линейным преобразованием класса* 2, когда $\sigma \neq 1$ и $(\sigma - 1)^2 = 0$.

Так как условия $x(\sigma - 1) = 0$ и $x\sigma = x$ эквивалентны, то легко видеть, что класс линейного преобразования σ тогда и только тогда равен 2, когда

$$\sigma \neq 1 \text{ и } A(\sigma - 1) \leqslant J^+(\sigma);$$

второе из этих условий эквивалентно тому, что σ индуцирует тождественное линейное преобразование фактор-пространства $A/J^+(\sigma)$. Последнее обстоятельство не в меньшей степени определяет значение линейных преобразований класса 2, чем то, что они удовлетворяют некоторому специальному уравнению.

Предложение 1. *Если* τ *— произвольное линейное преобразование и* σ *— линейное преобразование класса* 2, *то* $Z(\sigma) \leqslant Z(\tau)$ *тогда и только тогда, когда в центре тела* F *существуют такие числа* h *и* $k \neq 0$, *что* $\tau = k[h(\sigma - 1) + 1]$.

Здесь через t, где t — число из F, обозначено соответствующее этому числу отображение, при котором элемент x F-пространства A отображается на элемент tx того же пространства. Мы указывали выше, что это отображение тогда и только тогда будет линейным преобразованием, когда число t отлично от 0 и содержится в центре тела F.

Доказательство. Достаточность нашего условия очевидна; таким образом, нам нужно только доказать его необходимость. Пусть $Z(\sigma) \leqslant Z(\tau)$. Тогда, так как σ принадлежит $Z(\sigma)$, то σ содержится также и в $Z(\tau)$; следовательно,

$$\sigma\tau = \tau\sigma. \tag{1.1}$$

Используя полученное равенство, обычными методами нетрудно показать, что

$$[A(\sigma - 1)]\tau = A(\sigma - 1) \text{ и } J^+(\sigma)\tau = J^+(\sigma). \tag{1.2}$$

Так как $A(\sigma - 1) \leqslant J^+(\sigma)$, то, в силу принципа дополнения (гл. II, § 1), существуют такие подпространства U и V, что

$$J^+(\sigma) = A(\sigma - 1) \dotplus U, \quad A = J^+(\sigma) \dotplus V.$$

Заметим теперь, что $A(\sigma - 1) = V(\sigma - 1)$, ибо $J^+(\sigma)(\sigma - 1) = 0$, и что из равенства $v'(\sigma - 1) = v''(\sigma - 1)$, где v' и v'' — элементы из V, следует равенство $v' = v''$. Таким образом,

(1.3) σ 1 индуцирует линейное преобразование v линейного многообразия (F, V) на линейное многообразие $[F, A(\sigma - 1)]$.

Докажем теперь следующее утверждение.

(1.4) В центре тела F существует такое число $k \neq 0$, что $x\tau = kx$ для каждого x из $A(\sigma - 1)$.

Для того, чтобы доказать это утверждение, прежде всего заметим, что, согласно утверждению (1.2), τ индуцирует на $A(\sigma-1)$ линейное преобразование τ'. Если теперь ω — произвольное линейное преобразование F-пространства $A(\sigma-1)$, то существует, и притом только одно, такое линейное преобразование ω^* F-пространства A, что

$$x\omega^* = \begin{cases} x\omega & \text{для } x \text{ из } A(\sigma-1), \\ x & \text{для } x \text{ из } U, \\ x\nu\omega\nu^{-1} & \text{для } x \text{ из } V, \end{cases}$$

где, напомним, ν является линейным преобразованием F-пространства V на F-пространство $A(\sigma-1)$, естественно обладающим обратным линейным преобразованием. Так как элемент $x\omega^*$ для каждого x из $A(\sigma-1)$ принадлежит $A(\sigma-1)$ и линейное преобразование σ оставляет неподвижным каждый элемент подпространства $J^+(\sigma) = A(\sigma-1) \dotplus U$, то $y\omega^*\sigma = y\omega^* = y\sigma\omega^*$ для любого y из $J^+(\sigma)$. Далее, так как $x\omega^*$ для x из V принадлежит V и линейные преобразования ν и $\sigma-1$ на подпространстве V совпадают, то

$$x\omega^*\sigma = x\omega^*\nu + x\omega^* = x\nu\omega + x\omega^* = x(\sigma-1)\omega + x\omega^* = \\ = x(\sigma-1)\omega^* + x\omega^* = x\sigma\omega^*$$

для x из V; здесь мы воспользовались также тем, что ω и ω^* совпадают на подпространстве $A(\sigma-1)$. Тем самым показано, что $\omega^*\sigma = \sigma\omega^*$ и, следовательно, ω^* принадлежит $Z(\sigma) \leqslant Z(\tau)$. Но это означает, что линейные преобразования τ и ω^* перестановочны, а поэтому перестановочны и линейные преобразования τ' и ω. Таким образом, мы показали, что τ' содержится в центре группы $T[F, A(\sigma-1)]$; теперь утверждение (1.4) непосредственно следует из предложения 1 и замечания 1 (§ 1).

Пусть теперь ω — произвольное линейное преобразование линейного многообразия (F, U). Тогда существует, и притом только одно, такое линейное преобразование ω^* F-пространства A, что $u\omega^* = u\omega$ для u из U и $x\omega^* = x$ для x из $A(\sigma-1) \dotplus V$. Так как σ оставляет неподвижным каждый элемент из $A(\sigma-1) \dotplus U$, а ω^* оставляет неподвижным каждый элемент из $A(\sigma-1) \dotplus V$, то линейные преобразования σ и ω^* перестановочны; отсюда следует, что ω^* принадлежит $Z(\tau)$, т. е. $\tau\omega^* = \omega^*\tau$.

Этот результат используем сначала в случае, когда $\omega = -1$. Предварительно заметим, что элемент $u\tau$ для u из U принадлежит $J^+(\sigma) = A(\sigma-1) \dotplus U$; поэтому существуют такие элементы u', u'', содержащиеся соответственно в U и $A(\sigma-1)$, что $u\tau = u' + u''$.

Принимая это во внимание, мы получаем, что

$$-u'-u''=-u\tau=u(-1)^*\tau=u\tau(-1)^*=(u'+u'')(-1)^*=-u'+u''$$

и, следовательно, $u''=0$, поскольку характеристика тела F отлична от 2. Тем самым показано, что $U\tau\leqslant U$; отсюда и из того, что линейное преобразование τ отображает подпространства $A(\sigma-1)$ и $A(\sigma-1)\dotplus U=J^+(\sigma)$ на себя, следует равенство $U=U\tau$. Таким образом, τ индуцирует линейное преобразование F-пространства U, перестановочное с любым другим линейным преобразованием ω этого пространства, ибо легко можно построить линейное преобразование ω^* F-пространства A, индуцирующее на U линейное преобразование ω и перестановочное с τ. Отсюда, а также из предложения 1 и замечания 1 (§ 1) следует существование в центре тела F такого числа $k'\neq 0$, что $u\tau=k'u$ для каждого u из U.

Так как $\sigma\neq 1$, то $A(\sigma-1)\neq 0$; следовательно, в $A(\sigma-1)$ существует элемент $a\neq 0$. В подпространстве U выберем произвольный элемент $u\neq 0$[1]). Тогда, по принципу дополнения, $U=Fu\dotplus U'$. Существует, и притом только одно, такое линейное преобразование α F-пространства A, при котором $u\alpha=u+a$ и $x\alpha=x$ для каждого x из $A(\sigma-1)\dotplus U'\dotplus V$. Так как линейное преобразование σ отображает подпространство $A(\sigma-1)\dotplus U'\dotplus V$ в себя и оставляет неподвижным элемент a, то $\sigma\alpha=\alpha\sigma$; отсюда и из нашего общего предположения вытекает, что и $\tau\alpha=\alpha\tau$. Теперь, используя утверждение (1.4) и результат предыдущего абзаца, мы получаем, что

$$ka+k'u=a\tau+u\tau=(a+u)\tau=u\alpha\tau=u\tau\alpha=k'u\alpha=k'a+k'u$$

и, следовательно, $k=k'$, так как $a\neq 0$. Таким образом, принимая во внимание утверждение (1.4) и результат предыдущего абзаца, мы получаем следующее утверждение:

(1.5) $x\tau=kx$ для каждого x из $A(\sigma-1)\dotplus U=J^+(\sigma)$.

Поскольку число k отлично от 0 и содержится в центре тела F, можно построить линейное преобразование $\gamma=k^{-1}\tau$; очевидно, что $Z(\tau)=Z(\gamma)$. Заметим, кроме того, что, в силу (1.5), $J^+(\sigma)\leqslant J^+(\gamma)$. Так как линейные преобразования γ и σ перестановочны и так как γ оставляет неподвижным каждый элемент подпространства $A(\sigma-1)\leqslant J^+(\sigma)$, то

$$[x-x\gamma](\sigma-1)=x(\sigma-1)-x\gamma(\sigma-1)=x(\sigma-1)-x(\sigma-1)\gamma=0$$

для каждого x из A и, следовательно,

$$A(\gamma-1)\leqslant K(\sigma-1)=J^+(\sigma)\leqslant J^+(\gamma)=K(\gamma-1).$$

[1]) Если $U=0$, то утверждение (1.5), ради которого проводится настоящее рассмотрение, тривиально. — *Прим. перев.*

Но это означает, что линейное преобразование γ либо тождественное, либо класса 2.

Докажем теперь, что

(1.6) $Fx(\gamma-1)\leqslant Fx(\sigma-1)$ для каждого x из A.

Действительно, если x—произвольный элемент F-пространства A, то $x=x'+x''$, где $x'\in V$ и $x''\in J^+(\sigma)\leqslant J^+(\gamma)$. Отсюда следует, что $x(\sigma-1)=x'(\sigma-1)$ и $x(\gamma-1)=x'(\gamma-1)$; таким образом, справедливость утверждения (1.6) достаточно доказать для элементов подпространства V.

Предположим теперь, что в V существует такой элемент x, что элемент $y=x(\gamma-1)$ не содержится в $A(\sigma-1)$. Тогда, поскольку $A(\sigma-1)\leqslant J^+(\sigma)$,

$$J^+(\sigma)=A(\sigma-1)\dot{+}Fy\dot{+}Y,$$

где Y—некоторое подпространство. Существует, и притом только одно, такое линейное преобразование η F-пространства A, при котором $y\eta=-y$ и $a\eta=a$ для каждого a из $A(\sigma-1)\dot{+}Y\dot{+}V$. Тем же методом, каким мы несколько раз пользовались, легко проверить, что $\eta\sigma=\sigma\eta$ и поэтому $\eta\gamma=\gamma\eta$. Отсюда следует, что

$$-y=y\eta=x(\gamma-1)\eta=x\eta(\gamma-1)=x(\gamma-1)=y,$$

т. е. $y=0$, и мы пришли к противоречию с нашим предположением о том, что y не содержится в $A(\sigma-1)$. Тем самым показано, что $V(\gamma-1)\leqslant A(\sigma-1)$.

Пусть теперь x—такой элемент подпространства V, что элементы $x(\sigma-1)$ и $x(\gamma-1)$ линейно независимы. Оба эти элемента содержатся в $A(\sigma-1)$; поскольку они линейно независимы, легко построить линейное преобразование F-пространства $A(\sigma-1)$, оставляющее неподвижным элемент $x(\sigma-1)$ и отображающее $x(\gamma-1)$ на $-x(\gamma-1)$. Но, как было показано в процессе доказательства утверждения (1.4), это линейное преобразование F-пространства $A(\sigma-1)$ индуцируется таким линейным преобразованием $\varkappa$ F-пространства A, что $x\varkappa=x$ и $\varkappa\sigma=\sigma\varkappa$. Следовательно, $\varkappa$ перестановочно с τ и γ; отсюда вытекает, что

$$x(\gamma-1)=x\varkappa(\gamma-1)=x(\gamma-1)\varkappa=-x(\gamma-1).$$

Таким образом, $x(\gamma-1)=0$, что противоречит нашему предположению о линейной независимости элементов $x(\gamma-1)$ и $x(\sigma-1)$.

Если x—отличный от 0 элемент подпространства V, то и $x(\sigma-1)\neq 0$; из результата предыдущего абзаца следует линейная зависимость элементов $x(\gamma-1)$ и $x(\sigma-1)$. Но последнее свойство эквивалентно тому, что $Fx(\gamma-1)\leqslant Fx(\sigma-1)$, чем и завершается доказательство утверждения (1.6).

Если теперь x—произвольный элемент подпространства $A(\sigma-1)$, то $x\nu^{-1}$ есть однозначно определенный элемент из V,

а элемент $x\beta = x\nu^{-1}(\gamma - 1)$ принадлежит $A(\gamma - 1)$. Поэтому, в силу утверждения (1.6),

$$Fx\beta = Fx\nu^{-1}(\gamma - 1) \leqslant Fx\nu^{-1}(\sigma - 1) = Fx\nu^{-1}\nu = Fx;$$

здесь мы пользуемся также тем, что ν является отображением подпространства V на подпространство $A(\sigma - 1)$, индуцированным эндоморфизмом $\sigma - 1$. Таким образом, β является эндоморфизмом F-пространства $A(\sigma - 1)$, удовлетворяющим условиям предложения 3 (гл. III, § 1)[1]. Следовательно, в теле F существует такое число h, что $x\beta = hx$ для каждого x из $A(\sigma - 1)$. Если $h \neq 0$, то, поскольку $A(\sigma - 1) \neq 0$ и $(fx)\beta = f(x\beta)$ для каждого f из F и любого x из $A(\sigma - 1)$, h содержится в центре тела F. Рассмотрим теперь произвольный элемент d подпространства V. Его образ $d(\sigma - 1)$ содержится в $A(\sigma - 1)$. Поэтому

$$hd(\sigma - 1) = d(\sigma - 1)\beta = d(\sigma - 1)\nu^{-1}(\gamma - 1) = d(\gamma - 1).$$

Отсюда следует, что

$$A[h(\sigma - 1) - (\gamma - 1)] = [J^+(\sigma) + V][h(\sigma - 1) - (\gamma - 1)] = \\ = V[h(\sigma - 1) - (\gamma - 1)] = 0,$$

и поэтому $h(\sigma - 1) = \gamma - 1$. Таким образом,

$$\tau = k\gamma = k[h(\sigma - 1) + 1],$$

где h и $k \neq 0$ — числа, содержащиеся в центре тела F; тем самым предложение 1 полностью доказано.

Предложение 2. *Пусть σ — линейное преобразование класса 2 и σ' — такая инволюция, что $J^+(\sigma) = J^+(\sigma')$. Тогда следующие свойства линейного преобразования τ эквивалентны:*

(I) *В центре тела F существует такое число $h \neq 0$, что $\tau = h(\sigma - 1) + 1$.*

(II) *Класс линейного преобразования τ равен 2, и $Z(\sigma) = Z(\tau)$.*

(III) *В $Z_2(\sigma')$ существует такой элемент γ, что $\tau = \gamma^{-1}\sigma\gamma$.*

(IV) *Линейные преобразования σ и τ сопряжены в группе $T(F, A)$ всех линейных преобразований F-пространства A, и $Z(\sigma) \leqslant Z(\tau)$.*

Доказательство. Если справедливо свойство (I), то $\tau - 1 = h(\sigma - 1)$ и $\sigma - 1 = h^{-1}(\tau - 1)$. Так как число h принадлежит центру тела F, то $(\tau - 1)^2 = h^2(\sigma - 1)^2 = 0$, т. е. класс линейного преобразования τ равен 2. Кроме того, в силу предложения 1, $Z(\sigma) \leqslant Z(\tau) \leqslant Z(\sigma)$. Таким образом, из свойства (I) следует свойство (II). Обратно, если справедливо свойство (II), то, согласно предложению 1, в центре тела F существуют такие

[1]) Если $r[A(\sigma - 1)] = 1$ и $\beta \neq 0$, то β принадлежит центру группы $T[F, A(\sigma - 1)]$, т. е. в этом случае нужно воспользоваться замечанием 1 (§ 1). — *Прим. перев.*

числа h и k, что $\tau = k[h(\sigma-1)+1]$. Так как оба линейных преобразования τ и σ имеют класс 2 и числа h, k содержатся в центре тела F, то

$$0 = (\tau-1)^2 = [kh(\sigma-1)+k-1]^2 = 2k(k-1)h(\sigma-1)+(k-1)^2.$$

Полученное равенство эквивалентно равенству $(k-1)^2 = 2kh(1-k)(\sigma-1)$. Но σ — линейное преобразование класса 2; поэтому из последнего равенства следует, что $(k-1)^4 = 0$, т. е. $k = 1$. Тем самым доказана эквивалентность свойств (I) и (II).

Пусть теперь выполняются эквивалентные свойства (I) и (II). Через γ обозначим такое линейное преобразование F-пространства A, при котором $x\gamma = hx$ для x из $J^+(\sigma') = J^+(\sigma)$ и $x\gamma = x$ для x из $J^-(\sigma')$. Так как $h \neq 0$ и содержится в центре тела F, то, в силу предложения 2 (§ 2), γ принадлежит $Z_2(\sigma')$. Если x — произвольный элемент F-пространства A, то $x = x' + x''$, где $x' \in J^+(\sigma') = J^+(\sigma)$ и $x'' \in J^-(\sigma')$. Поэтому $x'(\sigma-1) = 0$ и, следовательно,

$$x\gamma^{-1}(\sigma-1)\gamma = (x'\gamma^{-1}+x''\gamma^{-1})(\sigma-1)\gamma = (h^{-1}x'+x'')(\sigma-1)\gamma =$$
$$= x''(\sigma-1)\gamma = hx''(\sigma-1) = h[x'+x''](\sigma-1) = hx(\sigma-1),$$

ибо $x''(\sigma-1)$ принадлежит $J^+(\sigma)$. Отсюда вытекает, что

$$\gamma^{-1}\sigma\gamma - 1 = \gamma^{-1}(\sigma-1)\gamma = h(\sigma-1) = \tau - 1, \text{ т. е. } \gamma^{-1}\sigma\gamma = \tau;$$

тем самым показано, что свойство (III) следует из (I) и (II) [1].

Предположим теперь, что справедливо свойство (III). Тогда существует такое линейное преобразование γ, принадлежащее $Z_2(\sigma')$, что $\tau = \gamma^{-1}\sigma\gamma$; в силу предложения 2 (§ 2), в центре тела F существуют такие отличные от 0 числа h' и h'', что

$$x\gamma = \begin{cases} h'x & \text{для } x \text{ из } J^+(\sigma') = J^+(\sigma), \\ h''x & \text{для } x \text{ из } J^-(\sigma'). \end{cases}$$

Так как $A(\sigma-1)$ содержится в $J^+(\sigma)$, то для элемента x из $J^-(\sigma')$

$$x\gamma^{-1}(\sigma-1)\gamma = h''^{-1}x(\sigma-1)\gamma = h''^{-1}h'x(\sigma-1),$$

а для элемента x из $J^+(\sigma') = J^+(\sigma)$ —

$$x\gamma^{-1}(\sigma-1)\gamma = 0 = h''^{-1}h'x(\sigma-1).$$

Следовательно, $\gamma^{-1}(\sigma-1)\gamma = h''^{-1}h'(\sigma-1)$, где $h''^{-1}h'$ — элемент из центра тела F. Таким образом, из свойства (III) следует свойство (I), и этим доказана эквивалентность свойств (I) — (III).

Если справедливы все три свойства (I) — (III), то справедливо, очевидно, и свойство (IV). Обратно, если справедливо свой-

[1] В действительности при выводе свойства (III) автор использовал лишь свойство (I). — *Прим. перев.*

ство (IV), то, поскольку τ сопряжено с линейным преобразованием σ класса 2, класс самого τ также равен 2. Теперь, проведя те же самые рассуждения, какие были использованы при доказательстве того, что свойство (I) следует из свойства (II), мы из включения $Z(\sigma) \leqslant Z(\tau)$ выведем справедливость свойства (I). Тем самым эквивалентность свойств (I) — (IV) полностью доказана.

Предложение 3. *Класс линейного преобразования σ тогда и только тогда равен 2 (или 1), когда существуют такие инволюции σ' и σ'', что $J^+(\sigma') = J^+(\sigma'')$ и $\sigma = \sigma'\sigma''$.*

Доказательство. Пусть существуют такие инволюции σ', σ'', что $J^+(\sigma') = J^+(\sigma'')$ и $\sigma = \sigma'\sigma''$. Положим $S = J^+(\sigma') = J^+(\sigma'')$. Если x — произвольный элемент F-пространства A, то существуют такие однозначно определенные элементы x' и x'', содержащиеся соответственно в $J^-(\sigma')$ и $J^-(\sigma'')$, что элементы $x - x'$ и $x - x''$ оба принадлежат S [ибо $A = S + J^-(\sigma') = S + J^-(\sigma'')$]. Но тогда

$$x\sigma' = (x - x')\sigma' + x'\sigma' = (x - x') - x' = 2(x - x') - x \equiv -x \pmod{S};$$

подобным же образом можно проверить, что $x\sigma'' \equiv -x \pmod{S}$. Следовательно, $x\sigma'\sigma'' \equiv x \pmod{S}$ для каждого x из A; в то же время для каждого элемента x из S имеет место, очевидно, равенство $x\sigma'\sigma'' = x$. Отсюда вытекает, что $A(\sigma'\sigma'' - 1) \leqslant S \leqslant J^+(\sigma'\sigma'')$; но это означает, что $\sigma = \sigma'\sigma''$ является линейным преобразованием класса 2 (или 1, если $\sigma = 1$).

Обратно, пусть σ есть линейное преобразование класса 2. Тогда $A(\sigma - 1) \leqslant J^+(\sigma)$. Существует такое подпространство V, что $A = J^+(\sigma) + V$; существует, далее, и притом только один такой эндоморфизм σ' F-пространства A, что

$$x\sigma' = \begin{cases} -x + x(\sigma - 1) & \text{для } x \text{ из } V, \\ x & \text{для } x \text{ из } J^+(\sigma). \end{cases}$$

Если x — элемент подпространства V, то

$$x\sigma'^2 = [-x + x(\sigma - 1)]\sigma' = -[-x + x(\sigma - 1)] + x(\sigma - 1) = x,$$

поскольку $x(\sigma - 1)$ принадлежит $J^+(\sigma)$. Отсюда вытекает, что $\sigma'^2 = 1$, т. е. σ' является инволюцией. Так как из $x(\sigma - 1) = 0$ для x из V следует $x = 0$, то $J^+(\sigma') = J^+(\sigma)$. Пусть теперь $\sigma'' = \sigma'\sigma$. Тогда для элемента x из V мы имеем

$$x\sigma'' = x\sigma'\sigma = [-x + x(\sigma - 1)]\sigma = -x\sigma + x(\sigma - 1) = -x,$$

поскольку $x(\sigma - 1)$ принадлежит $J^+(\sigma)$. Отсюда видно, что σ'' является такой однозначно определенной инволюцией, что $J^+(\sigma'') = J^+(\sigma)$ и $J^-(\sigma'') = V$. Таким образом, σ представлено нами в требуемом виде $\sigma = \sigma'\sigma''$; в действительности мы доказали более сильное утверждение, а именно

Следствие 1. *Если* σ *— линейное преобразование класса* 2, $A = J^+(\sigma) + V$ *и* σ'' *— такая однозначно определенная инволюция, что* $J^+(\sigma'') = J^+(\sigma)$ *и* $J^-(\sigma'') = V$, *то* $\sigma' = \sigma\sigma''$ *является инволюцией, для которой* $J^+(\sigma') = J^+(\sigma)$.

Мы подготовили все необходимое для того, чтобы дать мультипликативную характеристику линейных преобразований класса 2.

Теорема 1. *Класс линейного преобразования* σ *тогда и только тогда равен* 2, *когда* σ *обладает следующими свойствами:*

(а) *Линейное преобразование* τ *тогда и только тогда содержится в центре группы* $T(F, A)$, *когда* $Z(\sigma) < Z(\tau)$.

(б) *Совокупность* $Z^*(\sigma)$, *состоящая из* 1 *и тех линейных преобразований из центра подгруппы* $Z(\sigma)$, *которые сопряжены с* σ, *является подгруппой.*

(в) *Существует такая инволюция* σ', *что* $\sigma'\tau\sigma' = \tau^{-1}$ *для каждого* τ *из* $Z^*(\sigma)$.

(г) *Существует инволюция* α *и такое линейное преобразование* σ'', *принадлежащее второму централизатору* $Z_2(\alpha)$, *что* $\sigma''^{-1}\tau\sigma'' = \tau^2$ *для каждого* τ *из* $Z^*(\sigma)$.

(д) *Если порядок подгруппы* $Z^*(\sigma)$ *равен* 3, *то порядок центра группы* $T(F, A)$ *равен* 2.

Доказательство. Предположим сначала, что σ есть линейное преобразование класса 2. Сейчас мы выведем некоторые свойства централизатора $Z(\sigma)$, в которых содержатся перечисленные выше свойства (а) — (д); они идут, однако, несколько дальше и поэтому лучше описывают строение $Z(\sigma)$.

Прежде всего заметим, что, в силу предложения 1 (§ 1), σ, не будучи тождественным линейным преобразованием, не содержится в центре группы T; кроме того, $Z(\tau) = T$ тогда и только тогда, когда τ принадлежит центру группы T. Таким образом, если τ содержится в центре группы T, то $Z(\sigma) < Z(\tau)$. Обратно, пусть $Z(\sigma) < Z(\tau)$. Тогда, согласно предложению 1, в центре тела F существуют такие числа $k \neq 0$ и h, что $\tau = k[h(\sigma - 1) + 1]$. Если бы было $h \neq 0$, то $\sigma = h^{-1}[k^{-1}\tau - 1] + 1$ и, следовательно, $Z(\tau) \leqslant Z(\sigma)$, что невозможно. Таким образом, $h = 0$, и поэтому $\tau = k$ содержится в центре группы T. Тем самым необходимость условия (а) полностью доказана.

Если τ принадлежит центру подгруппы $Z(\sigma)$, то $Z(\sigma) \leqslant Z(\tau)$. Если, кроме того, τ сопряжено с σ, то τ удовлетворяет всем условиям предложения 2 (IV). Таким образом, в силу эквивалентности свойств (I) и (IV) предложения 2, справедливо следующее утверждение:

(А.1) $Z^*(\sigma)$ *является совокупностью всех линейных преобразований вида* $h(\sigma - 1) + 1$, *где* h *— число, принадлежащее центру тела* F.

Заметим, что при $h = 0$ мы получаем тождественное преобразование.

Пусть теперь h' и h'' — произвольные числа из центра тела F. Тогда, принимая во внимание, что $(\sigma-1)^2=0$, мы получаем, что

$$[h'(\sigma-1)+1][h''(\sigma-1)+1]=(h'+h'')(\sigma-1)+1$$

[из этого равенства, в частности, следует, что

$$[h(\sigma-1)+1]^{-1}=(-h)(\sigma-1)+1 \text{ и } \sigma^2=2(\sigma-1)+1].$$

В силу утверждения (А.1) и предыдущего равенства, справедливо следующее утверждение:

(А.2) *Отображение каждого числа h из центра тела F на линейное преобразование $h(\sigma-1)+1$ определяет изоморфное отображение аддитивной группы центра тела F на $Z^*(\sigma)$.*

Отсюда, в частности, вытекает, что $Z^*(\sigma)$ является подгруппой, содержащейся в центре подгруппы $Z(\alpha)$; кроме того, из утверждения (А.2) и предложения 1 (§ 1) непосредственно следует, что число отличных от 1 элементов подгруппы $Z^*(\sigma)$ равно числу элементов центра группы $T(F, A)$. Таким образом, доказана необходимость условий (б) и (д).

В силу следствия 1, существует такая инволюция σ', что $J^+(\sigma)=J^+(\sigma')=J^+(\sigma\sigma')$, причем $\sigma''=\sigma\sigma'$ также является инволюцией. Поэтому

$$\sigma'\sigma\sigma'=\sigma'\sigma''=(\sigma''\sigma')^{-1}=\sigma^{-1}.$$

С другой стороны, так как σ является линейным преобразованием класса 2, то $0=(\sigma-1)^2=\sigma^2-2\sigma+1$ и, следовательно,

$$(2-\sigma)\sigma=1, \text{ откуда } \sigma^{-1}=2-\sigma \text{ и } \sigma^{-1}-1=1-\sigma.$$

Если теперь h — произвольное число, принадлежащее центру тела F, то

$$\sigma'[h(\sigma-1)+1]\sigma'=h(\sigma'\sigma\sigma'-1)+1=h(\sigma^{-1}-1)+1=$$
$$=h(1-\sigma)+1=(-h)(\sigma-1)+1=[h(\sigma-1)+1]^{-1};$$

последнее равенство имеет место в силу утверждения (А.2). Таким образом, доказана необходимость условия (в).

Рассмотрим теперь некоторое число $h\neq 0$, принадлежащее центру тела F. Из выбора инволюции σ' и из предложения 2 следует существование в $Z_2(\sigma')$ такого линейного преобразования $\gamma=\gamma(h)$, что $\gamma^{-1}\sigma\gamma=h(\sigma-1)+1$. Если теперь z — любое число из центра тела F, то

$$\gamma^{-1}[z(\sigma-1)+1]\gamma=z(\gamma^{-1}\sigma\gamma-1)+1=zh(\sigma-1)+1.$$

Так как, в силу предложения 2, каждое γ из $Z_2(\sigma')$ трансформирует σ в линейное преобразование вида $h(\sigma-1)+1$, где $h\neq 0$ и принадлежит центру тела F, то, используя предыдущее равенство, легко убедиться в справедливости следующих утверждений.

(А.3) *Для каждого отличного от* 0 *числа* h, *принадлежащего центру тела* F, *в* $Z_2(\sigma')$ *существует такое* γ, *что* $\gamma^{-1}\tau\gamma = h(\tau-1)+1$ *для любого* τ *из* $Z^*(\sigma)$; *обратно, для каждого* γ *из* $Z_2(\sigma')$ *в центре тела* F *существует такое число* $h \neq 0$, *что* $\gamma^{-1}\tau\gamma = h(\tau-1)+1$ *для любого* τ *из* $Z^*(\sigma)$.

Если применить первую часть утверждения (А.3) к частному случаю, когда число $h=2$ (оно отлично от 0, поскольку характеристика тела F отлична от 2), и принять во внимание, что класс каждого линейного преобразования $\tau \neq 1$ из $Z^*(\sigma)$ равен 2, то мы найдем такое линейное преобразование $\gamma = \gamma(2)$, принадлежащее $Z_2(\sigma')$, что

$$\gamma^{-1}\tau\gamma = 2(\tau-1)+1 = (\tau-1)^2+2(\tau-1)+1 = \tau^2$$

для каждого τ из $Z^*(\sigma)$. Тем самым доказана необходимость условия (г).

(А.4) $Z(\sigma)\cap Z_2(\sigma')$ *совпадает с центром группы* T, *а* $Z(\sigma)Z_2(\sigma')$ *является нормализатором подгруппы* $Z(\sigma)$ *в группе* T.

Нормализатор подгруппы состоит из всех элементов группы T, трансформирующих данную подгруппу в себя. Утверждение (А.4) легко следует из предложения 2 § 2 и предложения 2 настоящего параграфа. Детали доказательства мы опускаем, так как это утверждение использовать не будем.

Предположим теперь, что линейное преобразование σ удовлетворяет условиям (а) – (д). В силу условия (а), σ не принадлежит центру группы T.

Согласно условию (г), существует линейное преобразование γ, обладающее следующими свойствами:

(г.1) существует такая инволюция α, что γ принадлежит $Z_2(\alpha)$;

(г.2) $\gamma^{-1}\tau\gamma = \tau^2$ для каждого τ из $Z^*(\sigma)$.

Из свойства (г.1) и следствия 2 (§ 2) вытекает справедливость следующего утверждения:

(г.3) $$r\Big(\sum_{i=0}^{\infty} Fx\gamma^i\Big) \leqslant 2 \text{ и } \Big(\sum_{i=0}^{\infty} Fx\gamma^i\Big)\gamma = \sum_{i=0}^{\infty} Fx\gamma^i.$$

Докажем теперь, что

(Б.1) для каждого элемента x F-пространства A и любого τ из $Z^*(\sigma)$ ранг $r\Big(\sum_{i=0}^{\infty} Fx\tau^i\Big)$ конечен и $\Big(\sum_{i=0}^{\infty} Fx\tau^i\Big)\tau = \sum_{i=0}^{\infty} Fx\tau^i$.

Действительно, пусть $X = \sum_{i=0}^{\infty} Fx\gamma^i$. В силу утверждения (г.3), $r(X) < 2$ и $X\gamma = X$. Отсюда следует, что $X\gamma^j = X$ для каждого положительного и отрицательного целого числа j. Так как τ является линейным преобразованием, то ранг подпространства $X\tau$ не больше 2. Если

$$X\tau = Fx' + Fx'',$$

то положим $X' = \sum_{i=0}^{\infty} Fx'\gamma^i$ и $X'' = \sum_{i=0}^{\infty} Fx''\gamma^i$. Вновь применяя утверждение (г.3), мы получаем, что ранги подпространств X' и X'' не больше 2 и что

$$X'\gamma = X', \quad X''\gamma = X''.$$

Поскольку $\sum_{i=0}^{\infty} X\tau\gamma^i \leqslant X' + X''$ и $X = X\gamma^{-i}$, совокупность элементов $x\gamma^{-i}\tau\gamma^i = x\tau^{2^i}$ для $0 \leqslant i$ содержится в подпространстве $X' + X''$, ранг которого не превышает 4. Следовательно, элементы $x\tau^{2^i}$ линейно зависимы, а тем самым линейно зависимо и множество элементов $x, x\tau, \ldots, x\tau^j, \ldots$; этим доказано существование соотношения

$$x\tau^k = \sum_{j=0}^{k-1} c_j x\tau^j, \text{ где } c_j \text{ — числа из } F.$$

Отсюда следует, что ранг подпространства $\sum_{i=0}^{\infty} Fx\tau^i = V$ конечен (он не больше k); очевидно также, что $(\sum_{i=0}^{\infty} Fx\tau^i)\tau \leqslant \sum_{i=0}^{\infty} Fx\tau^i$. Так как τ является линейным преобразованием, то подпространства V и $V\tau$ имеют один и тот же конечный ранг; теперь из включения $V\tau \leqslant V$ и формулы для ранга (а) (гл. II, § 2) вытекает, что $V = V\tau$. Таким образом, утверждение (Б.1) доказано.

(Б.2) $J^-(\tau) = 0$ для каждого τ из $Z^*(\sigma)$.

Действительно, если элемент x принадлежит $J^-(\tau^{2^i})$ для некоторого неотрицательного числа i, то

$$x\tau^{2^i+1} = -x\tau^{2^i} = x$$

и, следовательно,

$$J^-(\tau^{2^i}) \leqslant J^+(\tau^{2^i+1}) \leqslant J^+(\tau^{2^j}) \text{ для всех } j > i.$$

Поскольку характеристика тела F отлична от 2, для любого линейного преобразования ν

$$J^+(\nu) \cap J^-(\nu) = 0;$$

принимая это во внимание, мы получаем, что

$$J^-(\tau^{2^i+1}) \cap \sum_{j=0}^{i} J^-(\tau^{2^j}) \leqslant J^-(\tau^{2^i+1}) \cap J^+(\tau^{2^i+1}) = 0.$$

Пусть теперь элемент $w \neq 0$ принадлежит $J^-(\tau)$. Тогда

$$w\gamma^i\tau^{2^i} = w\tau\gamma^i = -w\gamma^i \text{ для } i > 0;$$

таким образом, $w\gamma^i$ содержится в $J^-(\tau^{2^i})$. Поскольку ни один из элементов $w\gamma^i$ не равен 0, из установленного выше соотношения $J^-(\tau^{2^{i+1}}) \cap \sum_{j=0}^{i} J^-(\tau^{2^j}) = 0$ следует линейная независимость бесконечного множества элементов $w\gamma^i$, что противоречит утверждению (г.3). Таким образом, $J^-(\tau)$ не содержит ни одного отличного от 0 элемента, и этим утверждение (Б.2) доказано.

(Б.3) Если τ принадлежит $Z^*(\sigma)$, то $\tau+1$ будет линейным преобразованием F-пространства A.

Прежде всего заметим, что, в силу утверждения (Б.2), $K(\tau+1) = J^-(\tau) = 0$; следовательно, $\tau+1$ является линейным преобразованием F-пространства A на его подпространство $A(\tau+1)$. Пусть теперь x — произвольный элемент F-пространства A; образуем подпространство $X = \sum_{i=0}^{\infty} Fx\tau^i$. В силу утверждения (Б.1), ранг $r(X)$ конечен и $X\tau = X$. Отсюда следует, что $\tau+1$ индуцирует линейное преобразование подпространства X на содержащееся в нем подпространство $X(\tau+1)$. Так как эти два подпространства имеют один и тот же конечный ранг, то из формулы для ранга (а) вытекает, что $X(\tau+1) = X$. Таким образом, для каждого x из A подпространство $X = X(\tau+1)$ содержится в $A(\tau+1)$. Тем самым показано, что $A = A(\tau+1)$ и, следовательно, $\tau+1$ является линейным преобразованием F-пространства A.

(Б.4) $\tau + \tau^{-1} = 2$ для каждого τ из $Z^*(\sigma)$.

Действительно, утверждение очевидно, если $\tau = 1$; поэтому можно предположить, что $\tau \neq 1$. По условию (б), $Z^*(\sigma)$ содержит τ^2. Отсюда и из утверждения (Б.3) вытекает, что τ^2+1 является линейным преобразованием F-пространства A; следовательно, линейным преобразованием F-пространства A будет и сумма $\tau + \tau^{-1} = (\tau^2+1)\tau^{-1}$.

Поскольку τ содержится в центре подгруппы $Z(\sigma)$, мы имеем $Z(\sigma) \leqslant Z(\tau)$. Далее, так как линейные преобразования σ и τ сопряжены и σ не содержится в центре группы T, то и τ не содержится в центре группы T. Отсюда и из условия (а) вытекает, что $Z(\sigma) = Z(\tau)$.

Очевидно, что $Z(\tau) \leqslant Z(\tau+\tau^{-1})$. По условию (в), существует такая инволюция σ', что $\sigma'\tau\sigma' = \tau^{-1}$. Из условия (г) следует, что $\tau^2 \neq 1$, ибо в противном случае само $\tau = 1$. Отсюда вытекает, что $\tau \neq \tau^{-1}$ и σ' не содержится в централизаторе $Z(\tau)$. С другой стороны, так как σ' является инволюцией, то $\sigma'(\tau+\tau^{-1})\sigma' = \tau^{-1}+\tau$ и, следовательно, σ' содержится в централизаторе $Z(\tau+\tau^{-1})$. Тем самым показано, что

$$Z(\sigma) = Z(\tau) < Z(\tau+\tau^{-1}).$$

Отсюда и из условия (а) вытекает, что $\tau+\tau^{-1}$, будучи линейным преобразованием F-пространства A (т. е. элементом группы T), принадлежит центру группы T.

Рассмотрим теперь два случая.

Случай 1: порядок подгруппы $Z^*(\sigma)$ не равен 3. При этом условии в $Z^*(\sigma)$ существует элемент τ', отличный от 1, τ и τ^{-1} [подгруппа $Z^*(\sigma)$ непременно содержит указанные три попарно различных элемента]. По условию (б), элементы τ, τ', $\tau\tau'$ и $\tau\tau'^{-1}$ принадлежат подгруппе $Z^*(\sigma)$, а так как все эти элементы отличны от 1, то они попарно сопряжены в группе T. Поэтому

$$\tau+\tau^{-1},\ \tau'+\tau'^{-1},\ \tau\tau'+(\tau\tau')^{-1},\ \tau\tau'^{-1}+(\tau\tau'^{-1})^{-1}$$

являются попарно сопряженными элементами, содержащимися в центре группы T. Следовательно, эти элементы совпадают друг с другом; их общее значение, которое отлично от 1, обозначим через e; e есть отличный от 0 элемент из центра тела F. Используя теперь коммутативность подгруппы $Z^*(\sigma)$, мы получаем, что

$$e^2=(\tau+\tau^{-1})(\tau'+\tau'^{-1})=\tau\tau'+(\tau\tau')^{-1}+\tau\tau'^{-1}+(\tau\tau'^{-1})^{-1}=2e,$$

откуда $e=2$, что и требовалось доказать.

Случай 2: порядок подгруппы $Z^*(\sigma)$ равен 3. В этом случае $\tau^2=\tau^{-1}$ и, в силу условия (д), порядок центра группы T равен 2. Но, согласно предложению 2 (§ 1), центр группы T изоморфен мультипликативной группе центра тела F; следовательно, центр тела F состоит точно из 3 элементов. Значит, характеристика тела F равна 3. Поэтому для элемента $\tau+\tau^{-1}$, содержащегося в центре группы T, имеет место равенство

$$(\tau+\tau^{-1})^3=\tau^3+\tau^{-3}=2,$$

из которого следует, что $\tau+\tau^{-1}=2$, ибо центр тела F состоит лишь из 0, 1 и 2. Таким образом, утверждение (Б.4) полностью доказано.

Так как σ содержится в $Z^*(\sigma)$, то, в силу утверждения (Б.4), $\sigma+\sigma^{-1}=2$, откуда $\sigma^2-1=2\sigma$; последнее же равенство эквивалентно тому, что $(\sigma-1)^2=0$. Так как $\sigma\neq 1$, то, следовательно, нами полностью показано, что σ является линейным преобразованием класса 2.

Замечание 1. При изоморфном отображении σ группы $T(F, A)$ на группу $T(G, B)$ элементы из $T(F, A)$, удовлетворяющие условиям (а) – (д) теоремы 1, отображаются на элементы группы $T(G, B)$, удовлетворяющие тем же условиям. Таким образом, из теоремы 1 следует:

Образом линейного преобразования класса 2 при изоморфном отображении σ группы $T(F, A)$ на группу $T(G, B)$ является линейное преобразование класса 2.

Интересен вопрос, нельзя ли опустить некоторые из пяти условий (а)—(д) теоремы 1. До настоящего времени об этом почти ничего не известно. Поэтому представляет некоторый интерес указанное в теореме 2 необходимое и достаточное условие для того, чтобы класс данного линейного преобразования был равен 2, являющееся более простым по сравнению с пятью условиями теоремы 1, хотя и допускающее применение лишь в частных случаях.

Предложение 4. *Класс линейного преобразования σ тогда и только тогда равен* 2, *когда* σ *является линейным преобразованием конечного класса и выполняется условие* (а) *теоремы* 1.

Доказательство. Необходимость указанных условий очевидна (см. теорему 1). Пусть теперь σ удовлетворяет этим двум условиям. Тогда, очевидно, σ не содержится в центре группы T, так что, в частности, σ не является линейным преобразованием класса 1. Но так как σ — линейное преобразование конечного класса, то существует такое натуральное число m, что $m > 1$, $(\sigma-1)^{m-1} \neq 0$ и $(\sigma-1)^m = 0$.

Положим $\tau = 1+(\sigma-1)^{m-1}$. Тогда $\tau \neq 1$, но $(\tau-1)^2 = (\sigma-1)^{2m-2} = 0$, ибо $m \geqslant 2$. Отсюда $1 = (2-\tau)\tau$, и тем самым показано, что τ является линейным преобразованием класса 2. Следовательно, τ, в частности, не содержится в центре группы T.

Очевидно, что $Z(\sigma) \leqslant Z(\tau)$; отсюда и из условия (а) (теоремы 1), принимая во внимание, что τ не содержится в центре группы T, мы получаем равенство $Z(\sigma) = Z(\tau)$. Поскольку τ является линейным преобразованием класса 2, из последнего соотношения и предложения 1 следует существование в центре тела F таких чисел $k \neq 0$ и h, что

$$\sigma = k[h(\tau-1)+1] = k[h(\sigma-1)^{m-1}+1].$$

Умножая обе части этого равенства на $\sigma-1$ и принимая во внимание, что $(\sigma-1)^m = 0$, получаем

$$\sigma(\sigma-1) = k(\sigma-1), \text{ откуда } (\sigma-1)^2 = (k-1)(\sigma-1);$$

умножая обе части последнего равенства на $(\sigma-1)^{m-2}$, находим, что

$$0 = (\sigma-1)^m = (k-1)(\sigma-1)^{m-1}.$$

Таким образом, если бы число $k-1$, содержащееся в центре тела F, было отлично от 0, то было бы $(\sigma-1)^{m-1} = 0$. Следовательно, $k = 1$, и поэтому $(\sigma-1)^2 = (k-1)(\sigma-1) = 0$, т. е. σ является линейным преобразованием класса 2, что и требовалось доказать.

Замечание 2. Следует отметить, что условие «σ является линейным преобразованием конечного класса» является аддитивным условием и поэтому не может заменить мультипликативные условия (б)—(д) теоремы 1.

Теорема 2. *Если характеристика тела F равна простому числу p, то класс линейного преобразования σ F-пространства A тогда и только тогда равен 2, когда $\sigma^p = 1$ и выполняется условие* (а) *теоремы* 1.

Доказательство. Так как характеристика тела F равна простому числу p, то $(\sigma - 1)^p = \sigma^p - 1$. Поэтому $\sigma^p = 1$ тогда и только тогда, когда класс линейного преобразования σ не превышает p. Из этого замечания и предложения 4 непосредственно следует теорема 2.

§ 4. Смежные классы инволюций

Если S — подпространство линейного многообразия (F, A), то совокупность таких инволюций σ F-пространства A, что $S = J^+(\sigma)$, обозначим через $\Delta(S)^+$; аналогично, совокупность таких инволюций σ, что $S = J^-(\sigma)$, обозначим через $\Delta(S)^-$. В настоящем параграфе мы покажем, что такие системы Δ можно охарактеризовать в пределах группы Т в чисто мультипликативных терминах и что эти системы полностью определяют свойства проективной геометрии F-пространства A (т. е. структуры подпространств F-пространства A).

Прежде всего заметим, что $\Delta(S)^- = -\Delta(S)^+$. Каждая инволюция σ содержится в системах $\Delta[J^+(\sigma)]^+$ и $\Delta[J^-(\sigma)]^-$ и не содержится ни в какой другой системе подобного типа. Ради краткости мы будем совокупности $\Delta(S)^+$ и $\Delta(S)^-$ называть $\Delta^\pm$-системами и через $\Delta(S)$ обозначать пару $[\Delta(S)^+, \Delta(S)^-]$.

Введем теперь следующие *обозначения*, которыми в дальнейшем будем всюду пользоваться. Если Φ есть некоторое множество инволюций, то через Φ^2 обозначим совокупность линейных преобразований вида $\sigma'\sigma''$, где σ' и σ'' — инволюции из Φ; через $N\Phi$ обозначим совокупность инволюций σ, удовлетворяющих условию $\Phi = \sigma\Phi\sigma$. Заметим, что $N\Phi$ состоит из всех инволюций, содержащихся в так называемом нормализаторе множества Φ в группе Т.

Предложение 1. *Каждая $\Delta^\pm$-система Φ обладает следующими свойствами*:

(а) *Если α, β, γ принадлежат Φ, то и $\alpha\beta\gamma = \gamma\beta\alpha$ принадлежит Φ.*

(б) *Если α, β принадлежат Φ, то в Φ существует одна и только одна такая инволюция γ, что $\gamma^3\gamma = \alpha$.*

(в) *Инволюция σ тогда и только тогда принадлежит $N\Phi$, когда в Φ существует такая инволюция α, что $\alpha\sigma = \sigma\alpha$.*

(г) *Класс каждого линейного преобразования, содержащегося в Φ^2, равен 1 или 2.*

Доказательство. Если Φ является $\Delta^\pm$-системой, то $\Phi = \Delta(S)^+$ или $\Phi = \Delta(S)^-$, где S — некоторое подпространство

F-пространства A. Поскольку $\Delta(S)^- = -\Delta(S)^+$, без ущерба для общности можно предположить, что $\Phi = \Delta(S)^+$.

Докажем сначала, что

(а.1) *если* α, β, γ *принадлежат* Φ, *то* $\alpha\beta\gamma = \alpha - \beta + \gamma$.

Действительно, так как $S = J^+(\alpha) = J^+(\beta) = J^+(\gamma)$, то элементы $x + x\alpha$, $x + x\beta$ и $x + x\gamma$ содержатся в S для каждого x из A и поэтому остаются неподвижными при любой из инволюций α, β и γ. Отсюда следует, что

$$\begin{aligned} x(\alpha - \beta + \gamma) &= x\alpha - x\beta + x\gamma = (x + x\alpha) - (x + x\beta) + x\gamma = \\ &= [(x + x\alpha) - (x + x\beta) + x]\gamma = [x + x\alpha - x\beta]\gamma = \\ &= x + x\alpha - x\beta\gamma = (x + x\alpha)\beta\gamma - x\beta\gamma = x\alpha\beta\gamma, \end{aligned}$$

т. е. $\alpha - \beta + \gamma = \alpha\beta\gamma$.

Из утверждения (а.1) вытекает, что $\alpha\beta\gamma = \gamma\beta\alpha$ и, следовательно,

$$(\alpha\beta\gamma)^2 = \alpha\beta\gamma\gamma\beta\alpha = 1.$$

Если элемент x содержится в $J^+(\alpha\beta\gamma)$, то

$$x = x(\alpha + \gamma - \beta), \text{ откуда } x + x\beta = x\alpha + x\gamma;$$

тем самым показано, что элемент $x\alpha + x\gamma$ принадлежит S. Но

$$x\alpha + x\gamma = x + x\alpha + x\gamma - x;$$

так как $x + x\alpha$ содержится в S, то из полученного равенства следует, что S содержит $x\gamma - x$. Так как $x\gamma - x$ принадлежит также и $J^-(\gamma)$, то $x\gamma - x$ принадлежит пересечению подпространств $J^+(\gamma) = S$ и $J^-(\gamma)$, которое равно 0. Следовательно, $x = x\gamma$ содержится в S; отсюда уже ясно, что $S = J^+(\alpha\beta\gamma)$. Таким образом, свойство (а) полностью доказано.

Пусть теперь β, γ, η — такие инволюции из Φ, что $\gamma\beta\gamma = \eta\beta\eta$. Тогда, в силу утверждения (а.1), $2\gamma - \beta = 2\eta - \beta$ и, следовательно, $\gamma = \eta$; тем самым показано, что существует не более одной инволюции γ, удовлетворяющей свойству (б). Если α, β — инволюции из Φ, то положим $\gamma = (\alpha + \beta)/2$; из утверждения (а.1) следует, что

$$\gamma^2 = 4^{-1}(2 + \alpha\beta + \beta\alpha) = 4^{-1}[2 + (\alpha\beta\alpha + \beta)\alpha] = 4^{-1}[2 + (2\alpha - \beta + \beta)\alpha] = 1;$$

таким образом, γ является инволюцией. Очевидно, что $S \leqslant J^+(\gamma)$; если же x принадлежит $J^+(\gamma)$, то

$$4x = 2x + 2x\gamma = 2x + x(\alpha + \beta) = (x + x\alpha) + (x + x\beta)$$

содержится в S, поскольку первое слагаемое $x + x\alpha$ остается неподвижным при инволюции α, а второе слагаемое $x + x\beta$ остается неподвижным при инволюции β и, следовательно, каждое из этих слагаемых принадлежит S. Но одновременно с элементом $4x$ в подпространстве S содержится и элемент x; тем самым показано, что $S = J^+(\gamma)$, т. е. γ принадлежит Φ. Используя теперь

утверждение (а.1), мы получаем, что

$$\gamma\alpha\gamma = 2\gamma - \alpha = \alpha + \beta - \alpha = \beta,$$

чем полностью доказана справедливость свойства (б).

Предположим теперь, что σ содержится в $N\Phi$ и что α — некоторая инволюция из Φ. Тогда $\sigma\alpha\sigma$ принадлежит Φ и, в силу свойства (б), в Φ существует, и притом только одна, такая инволюция β, что $\sigma\alpha\sigma = \beta\alpha\beta$. Из утверждения (а.1) следует, что

$$\sigma\alpha\sigma = \beta\alpha\beta = 2\beta - \alpha.$$

Умножая это равенство слева и справа на инволюцию σ, мы получаем

$$\alpha = 2\sigma\beta\sigma - \sigma\alpha\sigma = 2\sigma\beta\sigma - \beta\alpha\beta = 2\sigma\beta\sigma - (2\beta - \alpha),$$

$$2\beta = 2\sigma\beta\sigma, \text{ откуда } \beta\sigma = \sigma\beta.$$

Этим доказана необходимость условия, сформулированного в свойстве (в).

Обратно, если σ — такая инволюция, что $\sigma\alpha = \alpha\sigma$ для некоторого α из Φ, то

$$S = J^+(\alpha) = J^+(\sigma\alpha\sigma) = J^+(\alpha)\sigma = S\sigma,$$

$$J^+(\sigma\beta\sigma) = S\sigma = S \text{ для каждого } \beta \text{ из } \Phi,$$

$$\sigma\Phi\sigma = \Phi,$$

поскольку $\Phi = \Delta(S)^+$. Тем самым свойство (в) полностью доказано.

Справедливость свойства (г) непосредственно следует из предложения 3 (§ 3).

Предложение 2. *Пусть некоторое множество* Φ *инволюций обладает свойствами* (а) — (г) *предложения* 1. *Тогда*:

(1) Φ^2 *является абелевой подгруппой группы* T.

(2) $\sigma\sigma'\sigma = \sigma'^{-1}$ *для каждого* σ *из* Φ *и каждого* σ' *из* Φ^2.

(3) *Если* Φ *содержит по крайней мере две инволюции, то либо* $\Phi \leqslant \Delta[J^+(\Phi^2)]^+$, *либо* $\Phi \leqslant \Delta[J^+(\Phi^2)]^-$ [1]).

Доказательство. Если σ', σ'' — элементы множества Φ^2, то в Φ существуют такие элементы $\alpha, \beta, \gamma, \delta$, что $\sigma' = \alpha\beta$ и $\sigma'' = \gamma\delta$. В силу свойства (а), $\alpha\beta\gamma$ принадлежит Φ. Отсюда следует, что $\sigma'\sigma'' = (\alpha\beta\gamma)\delta$ принадлежит Φ^2. Так как и $\sigma'^{-1} = \beta\alpha$ содержится в Φ^2, то нами доказано, что Φ^2 является подгруппой. Далее, из свойства (а) следует, что

$$\sigma'\sigma'' = \alpha\beta\gamma\delta = \gamma\beta\alpha\delta = \gamma\delta\alpha\beta = \sigma''\sigma'.$$

Таким образом, Φ^2 является абелевой подгруппой.

---

[1]) $J^+(\Phi^2)$ есть подпространство, состоящее из всех таких элементов x, что $x\sigma = x$ для каждого линейного преобразования σ из Φ^2.—*Прим. перев.*

Если σ, α, β — инволюции из Φ, то, используя свойство (а), мы получаем, что

$$\sigma\alpha\beta\sigma = \beta\alpha\sigma^2 = \beta\alpha = (\alpha\beta)^{-1},$$

и этим утверждение (2) доказано.

Покажем теперь, что

(3′) $$J^+(\Phi^2) \neq 0.$$

Действительно, в силу свойства (г), $(\sigma-1)^2=0$ для каждого линейного преобразования σ, принадлежащего Φ^2. Если σ' и σ'' оба принадлежат Φ^2, то из утверждения (1) вытекает, что $\sigma'\sigma'' = \sigma''\sigma'$ также содержится в Φ^2. Поэтому

$$0 = (\sigma'\sigma'' - 1)^2 = (\sigma'\sigma'')^2 - 2\sigma'\sigma'' + 1 = \sigma'^2\sigma''^2 - 2\sigma'\sigma'' + 1 =$$
$$= (2\sigma' - 1)(2\sigma'' - 1) - 2\sigma'\sigma'' + 1 = 2(\sigma'\sigma'' - \sigma' - \sigma'' + 1) =$$
$$= 2(\sigma' - 1)(\sigma'' - 1);$$

таким образом, $(\sigma'-1)(\sigma''-1)=0$ для любых σ', σ'' из Φ^2. Но отсюда следует, что

$$A(\sigma'-1) \leqslant K(\sigma''-1) = J^+(\sigma'') \text{ для любых } \sigma', \sigma'' \text{ из } \Phi^2.$$

Если для каждого σ из Φ^2 подпространство $A(\sigma-1)$ является нулевым, то Φ^2 состоит лишь из 1 и, следовательно, $J^+(\Phi^2) = A$; в противном случае из предыдущего включения вытекает, что

(3″) $$\sum_{\sigma \in \Phi^2} A(\sigma-1) \leqslant \prod_{\sigma \in \Phi^2} J^+(\sigma) = J^+(\Phi^2);$$

из полученного соотношения вытекает утверждение (3′), которое мы доказывали.

Пусть теперь σ принадлежит $N\Phi$. Тогда, как легко проверить, $\sigma\Phi^2\sigma = \Phi^2$, так что инволюция σ содержится и в $N\Phi^2$. Отсюда следует, что

(4′) $J^+(\Phi^2) = J^+(\sigma\Phi^2\sigma) = J^+(\Phi^2)\,\sigma$ для каждой инволюции σ из $N\Phi$.

Рассмотрим теперь произвольную инволюцию α из Φ. Если τ — такая инволюция, что $\tau\alpha = \alpha\tau$, то, в силу свойства (в) предложения 1, τ содержится в $N\Phi$; отсюда и из равенства (4′) вытекает, что $J^+(\Phi^2)\,\tau = J^+(\Phi^2)$ для каждой инволюции τ из централизатора $Z(\alpha)$. Воспользовавшись теперь предложением 3 (§ 2), мы получаем, что

(4″) $J^+(\Phi^2)$ равно либо 0, либо $J^+(\alpha)$, либо $J^-(\alpha)$, либо A для каждого α из Φ.

В силу утверждения (3′), $J^+(\Phi^2) \neq 0$. Если $J^+(\Phi^2) = A$, то Φ^2 будет единичной подгруппой, и, следовательно, Φ состоит лишь из одной инволюции; но этот случай мы теперь исключаем

[см. дополнительное предположение, сделанное в формулировке утверждения (3)].

Допустим теперь, что $J^+(\Phi^2) = J^+(\alpha)$ для некоторой инволюции α из Φ. Если β — любая другая инволюция, принадлежащая Φ, то, в силу свойства (б) из предложения 1, в Φ существует такая инволюция γ, что $\beta = \gamma\alpha\gamma$. Так как каждая инволюция γ, содержащаяся в Φ, в силу свойства (а), содержится и в $N\Phi$, то мы можем воспользоваться теперь утверждением (4'), из которого следует, что

$$J^+(\beta) \leqq J^+(\gamma\alpha\gamma) = J^+(\alpha)\,\gamma = J^+(\Phi^2)\,\gamma = J^+(\Phi^2).$$

Таким образом, $\Phi \leqslant \Delta\,[J^+(\Phi^2)]^+$. Если же для каждой инволюции α, принадлежащей Φ, $J^+(\Phi^2) \neq J^+(\alpha)$, то из предыдущих рассмотрений [см. (4'')] вытекает, что $J^+(\Phi^2) = J^-(\alpha)$ для каждого α из Φ и, следовательно, $\Phi \leqslant \Delta\,[J^+(\Phi^2)]^-$. Этим утверждение (3) полностью доказано.

Мы теперь подготовлены к тому, чтобы дать мультипликативную характеристику $\Delta^{\pm}$-систем.

Теорема 1. *Множество Φ инволюций тогда и только тогда является $\Delta^{\pm}$-системой, когда Φ есть максимальная система, обладающая свойствами* (а) — (г) *предложения* 1.

Доказательство. Предположим сначала, что $\Phi = \Delta(S)^+$, где S — некоторое подпространство F-пространства A. Тогда, в силу предложения 1, Φ обладает свойствами (а) — (г). Допустим теперь, что существует множество Φ' инволюций, большее чем Φ и также обладающее свойствами (а) — (г). Положим $S' = J^+(\Phi'^2)$. Из $\Phi^2 \leqslant \Phi'^2$ следует, что $S' = J^+(\Phi'^2) \leqslant J^+(\Phi^2) = S$. Поскольку $\Phi < \Phi'$, Φ' содержит по крайней мере две инволюции; используя теперь утверждение (3) предложения 2, мы получаем, что либо $\Phi' \leqslant \Delta(S')^+$, либо $\Phi' \leqslant \Delta(S')^-$. Так как $\Phi < \Phi'$ и $S' \leqslant S$, то из справедливости включения $\Phi' \leqslant \Delta(S')^-$ следовало бы, что

$$J^-(\sigma) = S' \leqslant S = J^+(\sigma)$$

для каждой инволюции σ из Φ. Но это соотношение равносильно, очевидно, тому, что $J^-(\sigma) = 0$ и $\sigma = 1$. Поскольку, как было отмечено выше, Φ' содержит по крайней мере два элемента, в Φ' существует элемент, не сопряженный с $\sigma = 1$, что противоречит свойству (б). Таким образом, $\Phi' \leqslant \Delta(S')^+$. Тогда, поскольку каждая инволюция σ, принадлежащая Φ, принадлежит и Φ', мы получаем, что $S = J^+(\sigma) = S'$. Но отсюда следует, что

$$\Delta(S)^+ = \Phi < \Phi' \leqslant \Delta(S')^+ = \Delta(S)^+.$$

Тем самым мы пришли к противоречию, чем доказана максимальность множества Φ.

Обратно, пусть Φ — максимальное множество инволюций, удовлетворяющее условиям (а) – (г) предложения 1. Если Φ состоит лишь из 1, то $\Phi = \Delta(A)^+$; если же Φ состоит только из -1, то $\Phi = \Delta(A)^-$. Предположим теперь, что Φ состоит лишь из одной инволюции σ, причем $\sigma \neq \pm 1$. Тогда $0 \quad J^+(\sigma) < A$; легко построить такую инволюцию $\sigma' \neq \sigma$, что $J^+(\sigma') = J^+(\sigma)$. Следовательно, $\Phi < \Delta[J^+(\sigma)]^+ = \Phi'$; в силу предложения 1, множество Φ' инволюций также обладает свойствами (а) — (г) предложения 1. Но это противоречит максимальности множества Φ. Тем самым показано, что Φ тогда и только тогда содержит ровно одну инволюцию, когда Φ состоит лишь из 1 или -1. Допустим, наконец, что Φ содержит по крайней мере две инволюции. Тогда, в силу утверждения (3) предложения 2, либо $\Phi \leqslant \Delta(S)^+$, либо $\Phi \leqslant \Delta(S)^-$, где $S = J^+(\Phi^2)$. Но так как $\Delta^\pm$-системы обладают свойствами (а) – (г) предложения 1, то из максимальности множества Φ следует, что либо $\Phi = \Delta(S)^+$, либо $\Phi = \Delta(S)^-$, т. е. Φ является Δ-системой. Таким образом, наша теорема полностью доказана; попутно доказано и следующее утверждение.

Следствие 1. *Φ тогда и только тогда будет максимальной системой инволюций, обладающей свойствами* (а) – (г) *предложения* 1 *и содержащей только одну инволюцию, когда эта единственная инволюция является либо* 1, *либо* -1.

Мы будем говорить, что подпространство V *расположено между* подпространствами U и W, если $U \leqslant V \leqslant W$ или $W \leqslant V \leqslant U$. Ближайшая наша цель состоит в том, чтобы охарактеризовать соотношение «между» для подпространств в терминах соответствующих $\Delta^\pm$-систем. Решение этой задачи содержится в теореме 2, формулировке и доказательству которой мы предпошлем доказательства нескольких предложений.

Предложение 3. *Следующие свойства подпространств S и T F-пространства A эквивалентны:*

(I) $S \leqslant T$ *или* $T \leqslant S$.

(II) $\Delta(S)^+ \leqslant N\Delta(T)^+$.

(III) $\Delta(T)^+ \leqslant N\Delta(S)^+$.

Замечание. Так как $\Delta(X)^- = -\Delta(X)^+$, то, очевидно, в условиях (II) и (III) знак плюс можно было бы заменить знаком минус.

Доказательство. Пусть $S \leqslant T$. Если σ принадлежит $\Delta(S)^+$, то $S = J^+(\sigma)$; поэтому из $S \leqslant T$ и $A = J^+(\sigma) \dotplus J^-(\sigma)$ следует, что

$$T = S \dotplus [T \cap J^-(\sigma)].$$

Обозначим через U любое подпространство, удовлетворяющее условию

$$J^-(\sigma) = [T \cap J^-(\sigma)] \dotplus U,$$

а через σ' обозначим такую однозначно определенную инволюцию, что $T = J^+(\sigma')$ и $U = J^-(\sigma')$. Очевидно, что σ' принадлежит $\Delta(T)^+$; из предложения 1 (§ 2) следует, что $\sigma'\sigma = \sigma\sigma'$. Отсюда и из предложения 1 (в) вытекает, что σ содержится в $N\Delta(T)^+$. Таким образом, если $S \leqslant T$, то справедливо свойство (II). Далее, пусть τ — инволюция, принадлежащая $\Delta(T)^+$. Тогда $T = J^+(\tau)$. Существует такое подпространство V, что $T = S \dotplus V$. Через τ' обозначим единственную инволюцию, для которой

$$S = J^+(\tau'), \quad V \dotplus J^-(\tau) = J^-(\tau').$$

Очевидно, что τ' принадлежит $\Delta(S)^+$; в силу предложения 1 (§ 2), $\tau\tau' = \tau'\tau$. Отсюда и из предложения 1 (в) вытекает, что τ содержится в $N\Delta(S)^+$. Тем самым показано, что и свойство (III) следует из того же включения $S \leqslant T$. Заменяя включение $S \leqslant T$ включением $T \leqslant S$, мы точно так же сможем доказать, что из него следуют свойства (II) и (III). Таким образом, мы показали, что из свойства (I) следуют оба свойства (II) и (III).

Предположим теперь, что S не содержится в T и T не содержится в S. Тогда существуют такие отличные от 0 подпространства S' и T', что $S = (S \cap T) \dotplus S'$ и $T = (S \cap T) \dotplus T'$. Пусть s и t — отличные от 0 элементы, содержащиеся соответственно в S' и T'; через T'' обозначим некоторое подпространство, удовлетворяющее условию $T' = Ft \dotplus T''$. Обозначим, наконец, через W такое подпространство, что $A = (S + T) \dotplus W$. Тогда

$$A = (S \cap T) \dotplus S' \dotplus Ft \dotplus T'' \dotplus W = (S \cap T) \dotplus S' \dotplus F(t+s) \dotplus T'' \dotplus W,$$

ибо $t \neq 0$ и s принадлежит S'. Следовательно, существует, и притом только одна, такая инволюция ω, что $J^+(\omega) = S$, $J^-(\omega) = F(t+s) \dotplus T'' \dotplus W$. Очевидно, что ω принадлежит $\Delta(S)^+$. В то же время

$$t\omega = (t+s)\omega - s\omega = -(t+s) - s = -t - 2s$$

не содержится в T, так как $s \neq 0$ содержится в S', а следовательно, и в S, но не содержится в $S \cap T$. Таким образом, $T\omega \neq T$. Если теперь τ — инволюция из $\Delta(T)^+$, т. е. $T = J^+(\tau)$, то, в силу предложения 1 (§ 2), $\omega\tau \neq \tau\omega$. Отсюда и из предложения 1 (в) вытекает, что ω не содержится в $N\Delta(T)^+$; тем самым показано, что $\Delta(S)^+$ не содержится в $N\Delta(T)^+$. Таким образом, если не выполняется свойство (I), то не выполняется и свойство (II), т. е. свойство (I) является следствием свойства (II). Подобным же образом можно убедиться, что свойство (I) является следствием и свойства (III), чем завершается доказательство предложения 3.

Если S — произвольное подпространство F-пространства A и если инволюции σ', σ'' принадлежат $\Delta(S)^+$, то $-\sigma'$, $-\sigma''$ принадлежат $\Delta(S)^-$; кроме того, $\sigma'\sigma'' = (-\sigma')(-\sigma'')$. Отсюда следует, что

$$[\Delta(S)^+]^2 = [\Delta(S)^-]^2;$$

таким образом, представляется оправданным более короткое обозначение подгруппы $[\Delta(S)^+]^2$ через $\Delta(S)^2$.

Лемма 1. *Линейное преобразование σ тогда и только тогда принадлежит $\Delta(S)^2$, когда $A(\sigma - 1) \leqslant S \leqslant J^+(\sigma)$.*

Доказательство. Если σ содержится в $\Delta(S)^2$, то существуют такие инволюции σ', σ'', что $\sigma = \sigma'\sigma''$ и $S = J^+(\sigma') = J^+(\sigma'')$. Отсюда ясно, что $S \leqslant J^+(\sigma)$. Далее, так как для каждого x из A элементы $x + x\sigma'$ и $x + x\sigma''$ принадлежат соответственно $J^+(\sigma') = S$ и $J^+(\sigma'') = S$, то из равенства $x(\sigma - 1) = (x\sigma' + x)\sigma'' - (x\sigma'' + x)$ следует, что $A(\sigma - 1) \leqslant S$.

Обратно, пусть $A(\sigma - 1) \leqslant S \leqslant J^+(\sigma)$. Тогда существуют такие подпространства V и W, что $J^+(\sigma) = S \dotplus V$ и $A = J^+(\sigma) \dotplus W$. Существует одна и только одна такая инволюция σ'', для которой $J^+(\sigma'') = S$ и $J^-(\sigma'') = V \dotplus W$. Очевидно, что σ'' принадлежит $\Delta(S)^+$. Положим $\sigma' = \sigma\sigma''$. Тогда для любого x из A

$$x\sigma' = x\sigma\sigma'' = x(\sigma - 1)\sigma'' + x\sigma'' = x(\sigma - 1) + x\sigma'',$$

ибо $A(\sigma - 1) \leqslant S = J^+(\sigma'')$; следовательно, $\sigma' = \sigma + \sigma'' - 1$. Отсюда и из равенств $(\sigma - 1)^2 = 0$ и $\sigma''^2 = 1$ вытекает, что

$$\sigma'^2 = [(\sigma - 1) + \sigma'']^2 = (\sigma - 1)\sigma'' + \sigma''(\sigma - 1) + 1.$$

Используя соотношения

$$A(\sigma - 1) \leqslant S = J^+(\sigma'') = A(1 + \sigma'') \leqslant J^+(\sigma),$$

легко проверить, что $(\sigma - 1)\sigma'' = \sigma - 1$ и $(\sigma'' + 1)(\sigma - 1) = 0$; подставляя эти равенства в выражение для σ'^2, мы получаем $\sigma'^2 = 1$. Далее, очевидно, что $S \leqslant J^+(\sigma')$. Обратно, если элемент x принадлежит $J^+(\sigma')$, то $x = x\sigma' = x(\sigma + \sigma'' - 1)$, так что элемент $-x(\sigma - 1) = x(\sigma'' - 1)$ содержится в подпространстве $A(\sigma - 1) \cap \cap J^-(\sigma'') \leqslant S \cap (V + W) = 0$. Таким образом, $x = x\sigma''$, и, следовательно, x принадлежит $J^+(\sigma'') = S$; тем самым мы показали, что σ' содержится в $\Delta(S)^+$. Поэтому $\sigma = \sigma'\sigma''$ является элементом подгруппы $\Delta(S)^2$, что и требовалось доказать.

Замечание 1. Сравните формулировку и метод доказательства леммы 1 с предложением 3 и следствием 1 (§ 3).

Предложение 4. *Если S, T и X — подпространства F-пространства A, то*

(a) $0 = S \cap T$ *или* $A = S + T$ *тогда и только тогда, когда* $\Delta(S)^2 \cap \Delta(T)^2 = 1$;

(б) $0 < S \cap T \leqslant X \leqslant S+T < A$ *тогда и только тогда, когда*

$$1 < \Delta(S)^2 \cap \Delta(T)^2 \leqslant \Delta(X)^2.$$

Доказательство. Из леммы 1 непосредственно следует, что линейное преобразование σ тогда и только тогда принадлежит подгруппе $\Delta(S)^2 \cap \Delta(T)^2$, когда

$$A(\sigma - 1) \leqslant S \cap T \text{ и } S+T \leqslant J^+(\sigma).$$

Используя теперь эквивалентность следующих утверждений: $\sigma = 1$, $A(\sigma-1)=0$ и $J^+(\sigma)=A$, легко убедиться в справедливости утверждения (а).

При доказательстве утверждения (б) мы введем [эквивалентные в силу (а)] дополнительные предположения, что

$$0 < S \cap T, \; S+T < A \text{ и } \Delta(S)^2 \cap \Delta(T)^2 \neq 1.$$

Предположим сначала, что $S \cap T \leqslant X \leqslant S+T$. Тогда каждый элемент σ подгруппы $\Delta(S)^2 \cap \Delta(T)^2$ удовлетворяет условию

$$A(\sigma-1) \leqslant S \cap T \leqslant X \leqslant S+T \leqslant J^+(\sigma),$$

из которого, в силу леммы 1, следует, что σ принадлежит $\Delta(X)^2$. Тем самым необходимость нашего условия доказана. Пусть теперь $S \cap T$ не содержится в X. Тогда в подпространстве $S \cap T$ найдется элемент $w \neq 0$, не принадлежащий X. Так как $S+T < A$, то существует такая гиперплоскость H и такой элемент $a \neq 0$, что

$$S+T \leqslant H \text{ и } A = Fa \dotplus H.$$

Кроме того, существует, и притом только одно, такое линейное преобразование ω, при котором $x\omega = x$ для каждого x из H и $a\omega = a+w$. Так как

$$A(\omega-1) = Fw \leqslant S \cap T \leqslant S+T \leqslant H = J^+(\omega),$$

то ω принадлежит $\Delta(S)^2 \cap \Delta(T)^2$. Но $A(\omega-1)$ не содержится в X; отсюда и из леммы 1 следует, что ω не содержится в $\Delta(X)^2$. Пусть, наконец, X не содержится в $S+T$. Тогда в X существует элемент $y \neq 0$, не принадлежащий $S+T$. Обозначим через Y такое подпространство, что $A = (S+T) \dotplus Fy \dotplus Y$. Поскольку $S \cap T \neq 0$, в $S \cap T$ найдется элемент $z \neq 0$. Тогда существует одно и только одно такое линейное преобразование ν, при котором $x\nu = x$ для каждого x из $S+T+Y$ и $y\nu = y+z$. Как и в предыдущем случае, легко проверить, что ν содержится в пересечении подгрупп $\Delta(S)^2$ и $\Delta(T)^2$, но не содержится в подгруппе $\Delta(X)^2$, ибо $y \neq y\nu$ и, следовательно,

$$X \text{ не содержится в } J^+(\nu).$$

Таким образом, утверждение (б) полностью доказано.

Прежде чем формулировать дальнейшие результаты, несколько упростим наши *обозначения*. Так как $N\Delta(X)^+ = N\Delta(X)^-$, то эту совокупность инволюций мы обозначим через $N\Delta(X)$. Вспоминая, что в начале параграфа мы условились обозначать пару $[\Delta(X)^+, \Delta(X)^- = -\Delta(X)^+]$ через $\Delta(X)$, можно, используя введенное обозначение, записать условие (II) предложения 3 в более простом и в то же время более общем виде: $\Delta(S) \leqslant N\Delta(T)$.

Теорема 2. *Тогда и только тогда подпространства S, T и X F-пространства A отличны от 0 и A и подпространство X расположено между S и T, когда*

(а) $\Delta(S) \leqslant N\Delta(T)$ *или* $\Delta(T) \leqslant N\Delta(S)$;

(б) $1 < \Delta(S)^2 \cap \Delta(T)^2 \leqslant \Delta(X)^2$.

Доказательство. Пусть X расположено между S и T, и пусть ни одно из подпространств S, T не совпадает с 0 или A. Тогда мы можем предположить, что $0 < S \leqslant X \leqslant T < A$. Отсюда и из предложения 3 следует справедливость условия (а) и эквивалентность содержащихся в этом условии включений. Так как в рассматриваемом случае $S = S \cap T$ и $T \neq S$, то, используя предложение 4 (б), мы убеждаемся в справедливости условия (б).

Обратно, пусть выполняются условия (а) и (б). Из условия (а) и предложения 3 вытекает, что либо $S \leqslant T$, либо $T \leqslant S$; без ограничения общности можно предположить, что $S \leqslant T$ и, следовательно, $S = S \cap T$, $T = S + T$. Тогда, в силу условия (б) и предложения 4 (б),

$$0 < S \cap T = S \leqslant X \leqslant S + T = T < A.$$

Таким образом, подпространство X расположено между подпространствами S и T, каждое из которых отлично от 0 и A.

Мы сопоставили каждому подпространству S F-пространства A определенный объект, образованный элементами группы $\mathrm{T}(F, A)$ и состоящий из основной системы

$$\Delta(S) = [\Delta(S)^+, \Delta(S)^-]$$

и производных от нее систем $\Delta(S)^2$ и $N\Delta(S)$. В теореме 1 мы полностью описали те объекты группы T, которые являются образами подпространств S при этом отображении Δ; в теореме 2 было показано, каким соотношениям между образами при отображении Δ соответствует соотношение «быть расположенным между» для подпространств. Теперь мы решим вопрос, в какой мере отображение Δ является взаимно однозначным.

Теорема 3. (а) *Следующие свойства* (I) – (IV) *подпространства S F-пространства A эквивалентны:*

(I) *S есть либо* 0, *либо A.*

(II) $\Delta(S) = [+1, -1]$.

(III) $\Delta(S)^2 = 1$.

(IV) $N\Delta(S)$ *состоит из всех инволюций, содержащихся в* T.

(б) *Если* $0 < S \leqslant A$, *то* $S = J^+[\Delta(S)^2]$.

(в) *Если* Φ *— максимальное множество инволюций, обладающее свойствами* (а) — (г) *предложения* 1, *то* $\Delta[J^+(\Phi^2)] = [\Phi, -\Phi]$.

Доказательство. Эквивалентность свойств (I) и (II) очевидна; также очевидно, что из свойства (II) следуют свойства (III) и (IV). Если выполнено свойство (III), то $\Delta(S)^+$ состоит лишь из одной инволюции σ; по теореме 1, $\Delta(S)^+$ является максимальной системой инволюций, обладающей свойствами (а) — (г) предложения 1; поэтому можно воспользоваться следствием 1, из которого вытекает, что $\sigma = \pm 1$. Таким образом, если справедливо свойство (III), то справедливо и свойство (II). Наконец, пусть выполняется свойство (IV). Тогда $\Delta(X) \leqslant N\Delta(S)$ для каждого подпространства X F-пространства A; отсюда и из предложения 3 вытекает, что для каждого подпространства X либо $S \leqslant X$, либо $X \leqslant S$. Но легко видеть, что подпространство S, обладающее последним свойством, является либо 0, либо A; таким образом, из свойства (IV) следует свойство (I). Этим утверждение (а) полностью доказано.

Пусть теперь подпространство $S \neq 0$. Если x — произвольный элемент F-пространства A, не принадлежащий S, то $A = S \dotplus Fx \dotplus X$, где X — некоторое подпространство (принцип дополнения). Выбирая теперь в $S \neq 0$ произвольный элемент $s \neq 0$, мы можем, поскольку и $x \neq 0$, представить A в виде прямой суммы $A = S \dotplus F(x+s) \dotplus X$. Следовательно, существует одно и только одно такое линейное преобразование σ, при котором $y\sigma = y$ для каждого y из $S \dotplus X$ и $x\sigma = x + s$. Очевидно, что $A(\sigma - 1) = Fs \leqslant S \leqslant J^+(\sigma)$; поэтому, в силу леммы 1, σ принадлежит $\Delta(S)^2$. Но так как $s \neq 0$, то $x\sigma \neq x$ и, следовательно, x не принадлежит $J^+[\Delta(S)^2]$. С другой стороны, из леммы 1 непосредственно вытекает, что $S \leqslant J^+[\Delta(S)^2]$. Таким образом, $S = J^+[\Delta(S)^2]$ для каждого подпространства $S \neq 0$, чем и завершается доказательство утверждения (б).

Наконец, справедливость утверждения (в) легко следует из утверждения (3) предложения 2, теоремы 1 и следствия 1.

Если Φ есть максимальная система инволюций, обладающая свойствами (а) — (г) предложения 1, то пару $[\Phi, -\Phi]$ мы можем назвать Δ-*системой*. Используя теоремы 1 и 3, легко убедиться в справедливости следующего основного утверждения.

Теорема 4. *Отображения* S *в* $\Delta(S)$ *и* $[\Phi, -\Phi]$ *на* $J^+(\Phi^2)$ *определяют взаимно обратные* (*и поэтому взаимно однозначные*) *соответствия между совокупностью всех отличных от* 0 *подпространств* F*-пространства* A *и совокупностью всех* Δ*-систем группы* $\mathrm{T}(F, A)$.

В заключение этого параграфа мы покажем, как Δ-система может быть восстановлена по определяемой ею подгруппе Δ^2.

Предложение 5. *Если* $0 < S < A$, *то инволюция* α *тогда и только тогда принадлежит* $\Delta(S)$, *когда* $\alpha\sigma\alpha = \sigma^{-1}$ *для каждого* σ *из* $\Delta(S)^2$.

Доказательство. Необходимость нашего условия непосредственно следует из предложения 2. Пусть теперь $\alpha\sigma\alpha = \sigma^{-1}$ для каждого σ из $\Delta(S)^2$. Предположим сначала, что $J^+(\alpha)$ не содержится в S. Тогда в $J^+(\alpha)$ найдется элемент $w \neq 0$, не принадлежащий S. Существует такое подпространство W F-пространства A, что $A = S \dotplus Fw \dotplus W$. Если s — произвольный элемент из S, то, поскольку $w \neq 0$, $A = S \dotplus F(w+s) \dotplus W$. Поэтому существует, и притом только одно, такое линейное преобразование σ F-пространства A, при котором $w\sigma = w + s$ и $x\sigma = x$ для каждого x из $S + W$. Очевидно, что

$$A(\sigma - 1) = Fs \leqslant S \leqslant S + W = J^+(\sigma).$$

Таким образом, в силу леммы 1, σ принадлежит $\Delta(S)^2$; отсюда и из нашего основного предположения следует, что $\alpha\sigma\alpha = \sigma^{-1}$. Принимая теперь во внимание, что w содержится в $J^+(\alpha)$ и $s\sigma = s$, поскольку s является элементом подпространства S, мы получаем

$$s = w(\sigma - 1) = w\alpha(\sigma^{-1} - 1)\alpha = w(1 - \sigma)\sigma^{-1}\alpha = -s\alpha.$$

Тем самым показано, что

если $J^+(\alpha)$ не содержится в S, то $S \leqslant J^-(\alpha)$;

точно так же можно проверить, что

если $J^-(\alpha)$ не содержится в S, то $S \leqslant J^+(\alpha)$.

Поскольку $0 < S < A$, из полученных двух утверждений легко следует, что S совпадает либо с $J^+(\alpha)$, либо с $J^-(\alpha)$, и поэтому α принадлежит $\Delta(S)$.

§ 5. Изоморфизмы полной линейной группы

Легко видеть эквивалентность следующих свойств линейного многообразия (F, A):

(I) Характеристика тела F равна простому числу p.

(II) $pA = 0$.

Поэтому мы можем характеристику тела F называть также характеристикой линейного многообразия (F, A). Приняв во внимание, что ± 1 являются единственными элементами тела F, квадраты которых равны 1, мы из предложения 2 (§ 1) выведем, что характеристика линейного многообразия (F, A) тогда и только тогда равна 2, когда в центре группы $\Gamma(F, A)$ содержится

лишь одна тождественная инволюция. Как и в предыдущих трех параграфах, в настоящем параграфе мы будем также предполагать, что характеристики рассматриваемых линейных многообразий отличны от 2; из только что сделанного замечания следует, что наше предположение эквивалентно требованию существования в центре группы T инволюции, отличной от тождественной.

Кроме того, мы будем предполагать, что ранги рассматриваемых нами линейных многообразий не меньше трех. Отметим, что так как подпространствами линейного многообразия (F, A), имеющего ранг 2, являются только 0, точки и само A, то в этом случае из $0 < S \leqslant T < A$. следует $S = T$. Принимая это во внимание и используя теорему 4 и предложение 4 (§ 4), нетрудно найти внутреннее свойство группы $T(F, A)$, эквивалентное нашему предположению, что $r(A) \geqslant 3$. Точно сформулировать это свойство мы предоставляем читателю.

Пусть нам даны линейные многообразия (F, A) и (G, B), каждое из которых имеет ранг, не меньший 3, и характеристику, отличную от 2. Нашей целью сейчас является нахождение необходимых и достаточных условий изоморфности их групп $T(F, A)$ и $T(G, B)$, а также в случае, когда эти группы изоморфны, описание всех изоморфных отображений одной из них на другую. Решение первой из поставленных задач содержится в следующем предложении.

Структурная теорема. *Группы* $T(F, A)$ *и* $T(G, B)$ *изоморфны тогда и только тогда, когда линейные многообразия* (F, A) *и* (G, B) *либо проективно эквивалентны, либо двойственны друг другу.*

Напомним, что в структурной теореме проективной геометрии (гл. III, § 1) указаны необходимые и достаточные условия для проективной эквивалентности двух линейных многообразий; в теореме о двойственных линейных многообразиях (гл. IV, § 1) даны необходимые и достаточные условия для того, чтобы два линейных многообразия были двойственны друг другу.

Справедливость сформулированной структурной теоремы будет следовать из результатов, которые мы получим в процессе изучения совокупности всех возможных изоморфных отображений группы $T(F, A)$ на группу $T(G, B)$. Это изучение мы начнем с конструирования некоторых специальных классов изоморфных отображений.

Прежде всего напомним, что группа $T(F, A)$ состоит из всех элементов кольца эндоморфизмов $P(F, A)$ линейного многообразия (F, A), обладающих в этом кольце обратными элементами. Другими словами, T *является группой единиц кольца* P (см. гл. V, § 1).

Индуцированные изоморфизмы 1-го рода. Пусть σ — изоморфное отображение кольца $P(F, A)$ на кольцо $P(?, B)$. При этом изоморфном отображении группа единиц $T(F, A)$ коль-

ца $P(F, A)$ отображается на группу единиц $T(G, B)$ кольца $P(G, B)$. Таким образом, σ индуцирует изоморфное отображение σ' группы $T(F, A)$ на группу $T(G, B)$; σ' мы будем называть *индуцированным изоморфным отображением первого рода*. [Изоморфные отображения кольца эндоморфизмов $P(F, A)$ мы изучали в § 4 гл. V.]

Индуцированные изоморфизмы 2-го рода. Пусть σ — инверсно изоморфное отображение кольца $P(F, A)$ на кольцо $P(G, B)$. Это инверсно изоморфное отображение индуцирует инверсно изоморфное отображение группы единиц $T(F, A)$ кольца $P(F, A)$ на группу единиц $T(G, B)$ кольца $P(G, B)$. Если теперь определить отображение σ' при помощи равенства

$$\tau^{\sigma'} = (\tau^{\sigma})^{-1} \text{ для каждого } \sigma \text{ из } T(F, A),$$

то легко проверить, что σ' будет изоморфным отображением группы $T(F, A)$ на группу $T(G, B)$; σ' мы будем называть *индуцированным изоморфным отображением второго рода*. [Инверсно изоморфные отображения кольца эндоморфизмов $P(F, A)$ мы изучали в § 5 гл. V.]

Индуцированными изоморфными отображениями не исчерпываются все изоморфные отображения, которые можно определить между изоморфными группами $T(F, A)$ и $T(G, B)$. Однако, как будет показано, любое изоморфное отображение группы $T(F, A)$ на группу $T(G, B)$ отличается от некоторого индуцированного изоморфного отображения лишь на некоторый довольно специальный автоморфизм группы $T(F, A)$; к построению автоморфизмов такого типа мы сейчас и приступаем.

Сингулярные автоморфизмы группы $T(F, A)$. Автоморфизм α группы $T(F, A)$ мы назовем *сингулярным*, если $\sigma^{\alpha}\sigma^{-1}$ принадлежит центру Z группы T для каждого линейного преобразования σ из T [такие автоморфизмы часто называют центральными автоморфизмами группы T].

(1) *Если α – сингулярный автоморфизм группы* T, *то отображение α^* каждого элемента σ из* T *на элемент $\sigma^{\alpha}\sigma^{-1}$ является гомоморфным отображением группы* T *в ее центр* Z.

Утверждение очевидно, поскольку

$$(\sigma'\sigma'')^{\alpha^*} = (\sigma'\sigma'')^{\alpha}(\sigma'\sigma'')^{-1} = \sigma'^{\alpha}\sigma''^{\alpha^*}\sigma'^{-1} = \sigma'^{\alpha^*}\sigma''^{\alpha^*},$$

ибо σ''^{α^*} принадлежит центру Z группы T.

(2) *Если η – гомоморфное отображение группы* T *в ее центр* Z, *то тогда и только тогда существует такой (сингулярный) автоморфизм α группы* T, *что $\alpha^* = \eta$, когда отображение элемента ζ из* Z *на элемент ζ^{η} является автоморфизмом центра* Z.

Необходимость сформулированного условия непосредственно следует из того, что каждый автоморфизм группы T индуцирует автоморфизм ее центра Z. Обратно, если наше условие выполнено,

то обозначим через ν автоморфизм, обратный к тому автоморфизму центра Z, при котором элемент ζ отображается на элемент $\zeta\zeta^{\eta}$. Тогда мы имеем

$$\zeta = \zeta^{\nu}\zeta^{\eta\nu} = \zeta^{\nu}\zeta^{\nu\eta}$$

для каждого ζ из Z. Обозначим теперь через α отображение группы T в себя, задаваемое равенством $\sigma^{\alpha} = \sigma\sigma^{\eta}$ для каждого σ из T, а через β — такое отображение группы T в себя, при котором $\sigma^{\beta} = \sigma\sigma^{-\eta\nu}$; определение отображения β корректно, поскольку η отображает группу T в ее центр Z. Легко проверить, что α и β являются эндоморфизмами группы T и что $\alpha\beta = \beta\alpha = 1$; следовательно, α является автоморфизмом группы T, причем таким, что $\alpha^{*} = \eta$.

Пример. Пусть F — поле комплексных чисел и (F, A) — линейное многообразие конечного ранга n. Каждое линейное преобразование σ этого линейного многообразия можно представить в виде матрицы n-го порядка над полем комплексных чисел, определитель которой не зависит от специального выбора представления линейных преобразований матрицами (см. гл. V, § 1). Таким образом, определитель линейного преобразования σ представляет собой однозначно определенное число из F; абсолютная величина $|\sigma|$ определителя является однозначно определенным положительным действительным числом. Положим $\sigma^{\eta} = |\sigma|^2$. Очевидно, что η является гомоморфным отображением группы T в мультипликативную группу положительных действительных чисел, которая, в свою очередь, изоморфна некоторой подгруппе центра Z группы T. Произвольное линейное преобразование, принадлежащее центру группы T, представляет собой умножение каждого элемента F-пространства A на фиксированное комплексное число c; определитель такого линейного преобразования равен c^n. Теперь читатель без труда проверит, что $c^{\eta} = |c|^{2n}$ и что поэтому η удовлетворяет условию утверждения (2). Следовательно, отображая каждое линейное преобразование σ в $\sigma^{\alpha} = \sigma|\sigma|^2$, мы получаем нетривиальный сингулярный автоморфизм группы T.

Мы покажем теперь, что этот сингулярный автоморфизм α перестановочен не с каждым индуцированным автоморфизмом первого рода. В самом деле, существует автоморфизм ω поля комплексных чисел F, не отображающий действительные числа в действительные числа (см. любую монографию по современной алгебре, в которой изложена теория формально действительных полей). Если выбрать определенное представление группы T невырожденными матрицами n-го порядка над полем комплексных чисел F, то каждое линейное преобразование, представленное матрицей (a_{ik}), можно отобразить на линейное преобразование, представленное матрицей (a_{ik}^{ω}); полученное так отображение является индуцированным автоморфизмом β первого рода группы T.

Очевидно, что

$$\sigma^{\beta\alpha} = \sigma^{\beta}\,|\,\sigma^{\beta}\,|^2,\quad \sigma^{\alpha\beta} = \sigma^{\beta}\,|\,\sigma\,|^{2\beta} = \sigma^{\beta}\,|\,\sigma\,|^{2\omega}.$$

Так как $|\sigma^{\beta}|^2$ всегда является положительным действительным числом, а число $|\sigma|^{2\omega}$ может не быть даже действительным, то из полученных равенств следует, что $\beta\alpha \neq \alpha\beta$.

Читатель без труда найдет другие примеры сингулярных автоморфизмов. Интересно решить проблему об описании всех сингулярных автоморфизмов данной группы или по крайней мере решить вопрос, каждая ли полная линейная группа обладает нетривиальным сингулярным автоморфизмом.

Исчерпывающее описание всех изоморфных отображений группы $\mathrm{T}(F, A)$ содержит следующая

Теорема об изоморфном отображении. *Каждое изоморфное отображение группы* $\mathrm{T}(F, A)$ *на группу* $\mathrm{T}(G, B)$ *можно одним и только одним способом представить в виде* $\sigma'\sigma''$, *где* σ' *– сингулярный автоморфизм группы* $\mathrm{T}(F, A)$ *и* σ'' *— индуцированное изоморфное отображение (первого или второго рода) группы* $\mathrm{T}(F, A)$ *на группу* $\mathrm{T}(G, B)$.

Доказательство этой основной теоремы будет проведено в несколько этапов; некоторые из них интересны сами по себе. Начнем с характеристики сингулярных автоморфизмов.

Предложение 1. *Следующие свойства автоморфизма* σ *группы* $\mathrm{T}(F, A)$ *эквивалентны:*

(I) σ *является сингулярным автоморфизмом.*

(II) σ *оставляет неподвижным каждое линейное преобразование класса* 2.

(III) $\Delta(S)^{\sigma} = \Delta(S)$ *для каждого подпространства* S F*-пространства* A.

Доказательство. Пусть σ — сингулярный автоморфизм группы $\mathbf{T}$. Тогда $\tau^* = \tau^{\sigma}\tau^{-1}$ для каждого τ из T принадлежит центру Z группы T. Так как отображение τ в τ^* является, в силу утверждения (1), гомоморфизмом группы T в ее центр Z, то для произвольных линейных преобразований α, β мы имеем $(\alpha^{-1}\beta\alpha)^* = (\alpha^*)^{-1}\beta^*\alpha^* = \beta^*$.

Если α — инволюция, то и α^{σ} будет инволюцией. Поэтому

$$1 = (\alpha^{\sigma})^2 = (\alpha\alpha^*)^2 = \alpha^2\alpha^{*2} = \alpha^{*2};$$

таким образом, если $\alpha^2 = 1$, то $\alpha^* = \pm 1$.

Рассмотрим теперь произвольное линейное преобразование ω класса 2. В силу предложения 3 (§ 3), существуют такие инволюции ω', ω'', что $J^+(\omega') = J^+(\omega'')$ и $\omega = \omega'\omega''$. Инволюции ω' и ω'' сопряжены в группе T [см., например, предложение 1 (б) (§ 4)]; отсюда и из замечаний, сделанных выше, вытекает, что $\omega'^* =$

$= \omega''^* = \pm 1$. Поэтому

$$\omega^\sigma = \omega'^\sigma \omega''^\sigma = \omega'\omega'^*\omega''\omega''^* = \omega'\omega'' = \omega.$$

Этим показано, что из свойства (I) следует свойство (II). Используя предложение 5 (§ 4), легко убедиться, что при выполнении свойства (II) выполняется и свойство (III).

Пусть, наконец, справедливо свойство (III). Тогда, если S — произвольное подпространство F-пространства A, то $[\Delta(S)^2]^\sigma = \Delta(S)^2$. Далее, если τ — линейное преобразование, то из леммы 1 (§ 4) вытекает, что $\Delta(S\tau)^2 = \tau^{-1}\Delta(S)^2\tau$. Следовательно, для каждого подпространства S и каждого линейного преобразования α

$$\Delta(S\alpha^\sigma)^2 = \alpha^{-\sigma}\Delta(S)^2\alpha^\sigma = \alpha^{-\sigma}[\Delta(S)^2]^\sigma\alpha^\sigma = [\alpha^{-1}\Delta(S)^2\alpha]^\sigma =$$
$$= [\Delta(S\alpha)^2]^\sigma = \Delta(S\alpha)^2.$$

Отсюда и из теоремы 3 (б) (§ 4) вытекает, что $S\alpha^\sigma = S\alpha$ для каждого подпространства S и любого линейного преобразования α. Поэтому линейное преобразование $\alpha' = \alpha^\sigma\alpha^{-1}$ удовлетворяет условию $S\alpha' = S$ для каждого подпространства S F-пространства A; следовательно, в силу предложения 1 (§ 1), каждое α' содержится в центре группы T, и потому σ является сингулярным автоморфизмом группы T. Таким образом, свойство (I) следует из свойства (III). Этим предложение 1 полностью доказано.

В дальнейшем нам понадобится лемма, устанавливающая связь между кольцом эндоморфизмов и группой линейных преобразований данного линейного многообразия. При формулировании этой леммы мы будем пользоваться обозначениями, введенными в § 2 гл. V. Заметим, кроме того, что через $J-1$ обозначается совокупность всех эндоморфизмов вида $j-1$, где j — элемент подмножества J кольца эндоморфизмов P.

Лемма 1. *Если S — подпространство линейного многообразия (F, A), причем $0 < S < A$, то*

(а) $\Delta(S)^2 - 1 = N(S) \cap Q(S)$.

(б) $L[N(S) \cap Q(S)] = Q(S)$.

(в) $R[N(S) \cap Q(S)] = N(S)$.

Доказательство. Эндоморфизм σ F-пространства A тогда и только тогда принадлежит пересечению $N(S) \cap Q(S)$, когда $A\sigma \leqslant S \leqslant K(\sigma)$. В этом случае $\sigma^2 = 0$ и, следовательно,

$$(1+\sigma)(1-\sigma) = 1 - \sigma^2 = 1.$$

Таким образом, $1+\sigma$ является линейным преобразованием класса 2; из леммы же 1 (§ 4) следует, что $1+\sigma$ принадлежит $\Delta(S)^2$. Подобным же образом, используя лемму 1 (§ 4), нетрудно проверить, что каждый эндоморфизм вида $\tau - 1$, где $\tau \in \Delta(S)^2$, принадлежит $N(S) \cap Q(S)$. Тем самым утверждение (а) доказано.

Используя теперь предложение 2 (гл. V, § 2) и теорему 3 (б) (§ 4), мы получаем

$$L[N(S)\cap Q(S)] = Q(K[N(S)\cap Q(S)]) = Q(K[\Delta(S)^2 - 1]) = \\ = Q(J^+[\Delta(S)^2]) = Q(S),$$

чем доказано утверждение (б).

Так как $S < A$, то из леммы 1 (§ 4) легко вывести, что

$$S = A[\Delta(S)^2 - 1];$$

отсюда и из утверждения (а) вытекает, что $S = A[N(S)\cap Q(S)]$. Теперь, вновь воспользовавшись предложением 2 (гл. V, § 2), мы получаем, что

$$N(S) = N(A[N(S)\cap Q(S)]) = R[N(S)\cap Q(S)],$$

и этим утверждение (в) доказано.

Предложение 2. *Лишь тождественный автоморфизм группы* $\mathrm{T}(F, A)$ *одновременно является сингулярным и индуцированным (первого или второго рода) автоморфизмом.*

Доказательство. Если σ — сингулярный автоморфизм группы T, то, в силу предложения 1,

$$\Delta(S)^2 = [\Delta(S)^2]^\sigma \tag{2.1}$$

для каждого подпространства S F-пространства A.

Допустим теперь, что существует автоморфизм α кольца $\mathrm{P}(F, A)$, индуцирующий σ. Тогда для $0 < S < A$ мы получим, в силу леммы 1 и равенства (2.1),

$$[N(S)\cap Q(S)]^\sigma = [\Delta(S)^2]^\tau - 1 = [\Delta(S)^2]^\sigma - 1 = \\ = \Delta(S)^2 - 1 = N(S)\cap Q(S),$$

$$Q(S)^\sigma = L[N(S)\cap Q(S)]^\alpha = L[(N(S)\cap Q(S))^\alpha] = \\ = L[N(S)\cap Q(S)] = Q(S),$$

ибо при автоморфизме левый аннулятор данного подмножества отображается на левый аннулятор образа этого подмножества. Отсюда и из следствия 1 (гл. V, § 4) вытекает, что $\alpha = 1$. Так как автоморфизм σ индуцируется автоморфизмом α, то и $\sigma = 1$.

Предположим теперь, что существует такой инверсный автоморфизм β кольца P, что

$$\tau^\sigma\tau^\beta = 1 \text{ для каждого } \tau \text{ из T}.$$

Тогда из леммы 1 и равенства (2.1), принимая при этом во внимание, что $\Delta(S)^2$ является подгруппой и, следовательно, в ней вместе с каждым элементом содержится и обратный ему элемент,

мы получаем для $0 < S < A$, что

$$[N(S) \cap Q(S)]^{\beta} = [\Delta(S)^2]^{\beta} - 1 = [\Delta(S)^2]^{-\sigma} - 1 = \Delta(S)^2 - 1 = N(S) \cap Q(S),$$

$$N(S)^{\beta} = [R[N(S) \cap Q(S)]]^{\beta} = L([N(S) \cap Q(S)]^{\beta}) = L[N(S) \cap Q(S)] = Q(S).$$

По лемме 2 (гл. V, § 5), отображение подпространства S F-пространства A на подпространство $AN(S)^{\beta} = AQ(S)$ того же пространства является автодуальным отображением F-пространства A. Но из предложения 1 (гл. V, § 2) следует, что $S = AQ(S)$; таким образом, построенное выше автодуальное отображение оставляет неподвижным каждое подпространство F-пространства A, отличное от 0 и A, что, очевидно, невозможно, поскольку $r(A) > 2$. Тем самым предложение 2 полностью доказано. В действительности мы доказали более сильное утверждение, а именно

Следствие 1. *Тождественный автоморфизм является единственным автоморфизмом кольца* $\mathrm{P}(F, A)$, *индуцирующим сингулярный автоморфизм группы* $\mathrm{T}(F, A)$, *и ни один индуцированный автоморфизм второго рода не является сингулярным.*

Установим, наконец, связь между проективными и дуальными отображениями, с одной стороны, и специального рода отображениями, сохраняющими соотношение «расположения между», которые встретятся нам в процессе наших рассмотрений, с другой.

Лемма 2. *Пусть взаимно однозначное отображение* σ *совокупности отличных от* 0 *и* A *подпространств линейного многообразия* (F, A) *на совокупность отличных от* 0 *и* B *подпространств линейного многообразия* (G, B) *сохраняет соотношение «расположения между». Тогда* σ *индуцируется либо проективным, либо дуальным отображением.*

(Заметим, что трудности, возникающие при доказательстве утверждения, сформулированного в лемме 2, связаны с тем, что не определены значения 0σ и $A\sigma$; таким образом, основным вопросом здесь является следующий: всегда ли можно так доопределить значения 0σ и $A\sigma$, чтобы σ продолжало сохранять соотношение «расположения между».)

Доказательство. Если $0 < S \leqslant T < A$, то подпространство S расположено между подпространствами S и T. Поэтому подпространство $S\sigma$ расположено между подпространствами $S\sigma$ и $T\sigma$, т. е.

$$0 < S\sigma \leqslant T\sigma < B \text{ или } 0 < T\sigma \leqslant S\sigma < B.$$

Заметим теперь, что подпространство (отличное от 0 и всего пространства) тогда и только тогда будет точкой или гипер-

плоскостью, когда не существуют такие подпространства, отличные от 0 и всего пространства, что данное подпространство расположено строго между ними. Отсюда следует, что σ отображает точки на точки или гиперплоскости, а гиперплоскости — на гиперплоскости или точки. Рассмотрим два случая.

Случай 1: в F-пространстве A существует такая точка P, что ее образ $P\sigma$ является точкой. Если H — гиперплоскость, проходящая через точку P, то $H\sigma \neq P\sigma$ и $H\sigma$ либо содержится в $P\sigma$, либо само содержит $P\sigma$. Но так как $P\sigma$ является точкой, то она не содержит никаких других подпространств, кроме 0 и $P\sigma$; отсюда следует, что $P\sigma < H\sigma$. Таким образом, $H\sigma$ не является точкой, и поэтому $H\sigma$ будет гиперплоскостью G-пространства B, проходящей через точку $P\sigma$.

Пусть теперь Q — произвольная точка F-пространства A. Так как $r(A) > 2$, то в A существует гиперплоскость H, проходящая через P и Q. Из результата, полученного в предыдущем абзаце, вытекает, что $H\sigma$ будет гиперплоскостью G-пространства B. Но отсюда, проведя рассуждения, двойственные к тем, какими мы пользовались в предыдущем абзаце, легко показать, что $Q\sigma$ будет точкой, лежащей на гиперплоскости $H\sigma$. Таким образом, мы установили, что σ отображает точки на точки и гиперплоскости на гиперплоскости.

Пусть теперь $0 < S \leqslant T < A$. Тогда существует такая точка V, что $V \leqslant S$. Отсюда и из наших предположений следует, что $S\sigma$ расположено между $V\sigma$ и $T\sigma$. Но, как было показано выше, $V\sigma$ является точкой; поэтому $0 < V\sigma \leqslant S\sigma \leqslant T\sigma$. Таким образом, σ сохраняет соотношение порядка; отсюда следует, что σ индуцируется проективным отображением F-пространства A на G-пространство B.

Случай 2: в A существует такая точка Q, образ которой $Q\sigma$ не является точкой. Из результата, полученного при рассмотрении случая 1, следует, что в случае 2 образ $X\sigma$ любой точки X F-пространства A не будет точкой; отсюда видно, что σ отображает точки на гиперплоскости и гиперплоскости на точки. Пусть теперь $0 < S \leqslant T < A$. Тогда существует такая точка V, что $V \leqslant S$. Так как $V\sigma$ является гиперплоскостью и подпространство $S\sigma$ расположено между подпространствами $V\sigma$ и $T\sigma$, то $T\sigma \leqslant S\sigma \leqslant V\sigma$. Следовательно, σ индуцируется дуальным отображением, что и требовалось доказать.

Доказательство теоремы об изоморфном отображении. Пусть σ — изоморфное отображение группы $\mathrm{T}(F, A)$ на группу $\mathrm{T}(G, B)$. В силу замечания 1 (§ 3), σ отображает линейные преобразования класса 2 на линейные преобразования класса 2. Поэтому каждая система Φ инволюций из группы $\mathrm{T}(F, A)$, обладающая свойствами (а) — (г) из предложения 1 (§ 4), отображается на систему Φ^σ инволюций, обладающую теми же свойствами. Отсюда

и из теоремы 1 (§ 4) следует, что σ отображает Δ-системы группы $\mathrm{T}(F, A)$ на Δ-системы группы $\mathrm{T}(G, B)$.

Пусть теперь S — произвольное отличное от 0 и A подпространство F-пространства A. Образуем Δ-систему $\Delta(S)$; эту Δ-систему отобразим на Δ-систему $\Delta(S)^\sigma$ группы $\mathrm{T}(G, B)$. Последнюю отобразим на подпространство

$$S^\nu = J^+([\Delta(S)^\sigma]^2)$$

G-пространства B; из теоремы 4 (§ 4) [и того факта, что σ является взаимно однозначным отображением группы $\mathrm{T}(F, A)$ на всю группу $\mathrm{T}(G, B)$] следует, что ν будет взаимно однозначным отображением совокупности отличных от 0 и A подпространств F-пространства A на совокупность отличных от 0 и B подпространств G-пространства B. По теореме 2 (§ 4), ν сохраняет соотношение «расположения между»; отсюда и из леммы 2 вытекает, что ν индуцируется либо проективным, либо дуальным отображением, которое мы также обозначим через ν. Заметим, что, в силу теоремы 3 (в) (§ 4),

$$\Delta(S^\nu) = \Delta(S)^\sigma \text{ для } 0 < S < A.$$

Случай 1: ν — проективное отображение. В силу первой основной теоремы проективной геометрии (гл. III, § 1), проективное отображение ν индуцируется некоторым полулинейным преобразованием ω F-пространства A на G-пространство B, так что $S^\nu = S^\omega$. По лемме 3 (гл. V, § 4), полулинейное преобразование ω индуцирует также изоморфное отображение σ'' кольца эндоморфизмов $\mathrm{P}(F, A)$ на кольцо эндоморфизмов $\mathrm{P}(G, B)$, удовлетворяющее условиям

$$N(S)^{\sigma''} = \omega^{-1} N(S)\,\omega = N(S^\omega) = N(S^\nu),$$
$$Q(S)^{\sigma''} = \omega^{-1} Q(S)\,\omega = Q(S^\omega) = Q(S^\nu)$$

для каждого подпространства S F-пространства A. Отсюда и из леммы 1 следует, что

$$[\Delta(S)^2]^{\sigma''} - 1 = [\Delta(S)^2 - 1]^{\sigma''} = [N(S) \cap Q(S)]^{\sigma''} =$$
$$= N(S)^{\sigma''} \cap Q(S)^{\sigma''} = N(S^\nu) \cap Q(S^\nu) = \Delta(S^\nu)^2 - 1;$$

используя теперь теорему 4 (§ 4) [или предложение 5 (§ 4)], мы находим, что

$$\Delta(S)^{\sigma''} = \Delta(S)^\sigma$$

для каждого подпространства S, отличного от 0 и A. Поэтому, в силу предложения 1, $\sigma\sigma''^{-1} = \sigma'$ будет сингулярным автоморфизмом группы $\mathrm{T}(F, A)$. Таким образом, изоморфное отображение

$\sigma = \sigma'\sigma''$ разлагается в произведение сингулярного автоморфизма и изоморфного отображения первого рода, которое индуцируется изоморфным отображением σ'' кольца $P(F, A)$ на кольцо $P(G, B)$; однозначность такого разложения следует из предложения 2.

Случай 2: ν — дуальное отображение. В силу теоремы 2 (гл. V, § 5), ν индуцируется некоторым инверсно изоморфным отображением σ' кольца $P(F, A)$ на кольцо $P(G, B)$. Согласно лемме 2 (гл. V, § 5), это означает, что

$$S^{\nu} = K[Q(S)^{\sigma'}] = BN(S)^{\sigma'}$$

для каждого подпространства S F-пространства A. Так как при инверсно изоморфном отображении σ' правые аннуляторы отображаются на левые, а левые на правые, то из предыдущего равенства и предложения 4 (гл. V, § 2) следует, что

$$N(S^{\nu}) = Q(S)^{\sigma'},\ Q(S^{\nu}) = N(S)^{\sigma'}.$$

Отсюда, используя лемму 1, мы получаем, что

$$\Delta(S^{\nu})^2 - 1 = N(S^{\nu}) \cap Q(S^{\nu}) = Q(S)^{\sigma'} \cap N(S)^{\sigma'} = [Q(S) \cap N(S)]^{\sigma'} = [\Delta(S)^2 - 1]^{\sigma'} = [\Delta(S)^2]^{\sigma'} - 1.$$

Теперь из определения отображения ν и теоремы 4 (§ 4) [или предложения 5 (§ 4)] вытекает, что

$$\Delta(S)^{\sigma} = \Delta(S)^{\sigma'}$$

для каждого подпространства S, отличного от 0 и A.

Пусть σ'' — изоморфное отображение второго рода группы $T(F, A)$ на группу $T(G, B)$, индуцированное инверсно изоморфным отображением σ'. Тогда $\sigma\sigma''^{-1}$ будет автоморфизмом группы $T(F, A)$, оставляющим инвариантными все Δ-системы; в силу предложения 1, $\sigma\sigma''^{-1}$ будет сингулярным автоморфизмом группы $T(F, A)$. Таким образом, мы представили изоморфное отображение σ в виде произведения сингулярного автоморфизма и индуцированного изоморфного отображения второго рода; однозначность такого разложения вытекает из предложения 2. Этим теорема об изоморфном отображении полностью доказана.

Доказательство структурной теоремы. Если группы $T(F, A)$ и $T(G, B)$ изоморфны, то, согласно теореме об изоморфном отображении, существует либо изоморфное, либо инверсно изоморфное отображение кольца $P(F, A)$ на кольцо $P(G, B)$. Если кольца $P(F, A)$ и $P(G, B)$ изоморфны, то, в силу структурной теоремы (гл. V, § 4), линейные многообразия (F, A) и (G, B) имеют одно и то же строение, в частности, они проективно эквивалентны. Если же кольца $P(F, A)$ и $P(G, B)$ инверсно изоморфны, то, по лемме 2 (гл. V, § 5), существует дуальное отображение линейного многообразия (F, A) на линейное многообра-

зие (G, B) и, следовательно, эти линейные многообразия двойственны друг другу.

Обратно, из существования проективного отображения линейного многообразия (F, A) на линейное многообразие (G, B), по первой основной теореме проективной геометрии (гл. III, § 1), следует существование полулинейного преобразования F-пространства A на G-пространство B. В силу структурной теоремы (гл. V, § 4), это полулинейное преобразование индуцирует изоморфное отображение кольца $P(F, A)$ на кольцо $P(G, B)$, которое в свою очередь индуцирует изоморфное отображение группы $T(F, A)$ на группу $T(G, B)$. Если же существует дуальное отображение линейного многообразия (F, A) на линейное многообразие (G, B), то, по теореме 2 (гл. V, § 5), существует инверсно изоморфное отображение кольца $P(F, A)$ на кольцо $P(G, B)$, индуцирующее изоморфное отображение (второго рода) группы $T(F, A)$ на группу $T(G, B)$. Таким образом, структурная теорема полностью доказана.

ГРУППА АВТОМОРФИЗМОВ ГРУППЫ $T(F, A)$

Группа A автоморфизмов группы $T(F, A)$ имеет следующее строение. Она содержит подгруппу A_s всех сингулярных автоморфизмов; так как A_s состоит из тех и только тех автоморфизмов группы T, которые индуцируют тождественный автоморфизм фактор-группы T/Z [последняя группа изоморфна группе коллинеаций; см. гл. III, § 2, и предложение 1, § 1], то A_s является нормальным делителем группы A. Кроме того, в A содержится подгруппа A_i всех индуцированных автоморфизмов первого или второго рода. Используя следствие 1, легко проверить, что подгруппа A_i изоморфна группе всех автоморфизмов и инверсных автоморфизмов кольца $P(F, A)$; последнюю группу мы в § 5 гл. V называли «расширенной группой автоморфизмов кольца $P(F, A)$»; она, как было показано в §§ 4 и 5 гл. V, изоморфна группе автопроективных и автодуальных отображений исходного линейного многообразия (F, A). В силу теоремы об изоморфном отображении и следствия 1, группа A расщепляется на эти две подгруппы:

$$A = A_s A_i, \quad 1 = A_s \cap A_i.$$

Заметим, что в общем случае A_i не является нормальным делителем группы A, ибо если бы это было так, то каждый индуцированный автоморфизм группы T был бы перестановочен с каждым сингулярным автоморфизмом той же группы T; но мы построили выше пример, показывающий, что это не всегда имеет место.

Группа A_i содержит все внутренние автоморфизмы группы T. Они являются индуцированными автоморфизмами первого рода;

соответствующие им внутренние автоморфизмы кольца $P(F, A)$ индуцируются линейными преобразованиями. Группа A_i тогда и только тогда совпадает с группой внутренних автоморфизмов, когда тождественный автоморфизм является единственным автоморфизмом тела F (отсюда, в частности, следует, что F — поле) и ранг $r(A)$ бесконечен (так что F-пространство A не допускает дуальных отображений). Очевидно, что подгруппа внутренних автоморфизмов является нормальным делителем группы всех автоморфизмов группы T. Таким образом, в том частном случае, когда подгруппа A_i совпадает с группой внутренних автоморфизмов, группа A разлагается в прямое произведение группы внутренних автоморфизмов и группы сингулярных автоморфизмов. Детали доказательств высказанных здесь утверждений мы оставляем читателю.

Добавление I

Группы инволюций

Всякую подгруппу группы $T(F, A)$, состоящую только из инволюций, мы назовем *группой инволюций*. Некоторые авторы кладут это понятие в основу изучения изоморфных отображений группы T; см. работы Дьёдонне [1, 2, 3] и Макки [1]. Мы же при изучении изоморфных отображений группы T этим понятием не пользовались. В то же время группы инволюций имеют интересную связь с разложениями линейного многообразия (F, A) в прямую сумму его точек; именно эту связь мы и исследуем в настоящем добавлении. Как и в предыдущих параграфах, в этом добавлении мы будем предполагать, что характеристика тела F отлична от 2.

Лемма 1. *Множество* Ф *инволюций из группы* T *тогда и только тогда содержится в группе инволюций, когда* $\sigma'\sigma'' = \sigma''\sigma'$ *для любых* σ', σ'' *из* Ф.

Доказательство. Если Ф является частью группы инволюций, то $\sigma'\sigma''$ будет инволюцией для любых инволюций σ', σ'' из Ф. Но в таком случае

$$1 = (\sigma'\sigma'')^2 = \sigma'\sigma''\sigma'\sigma'', \text{ откуда } \sigma'\sigma'' = \sigma''^{-1}\sigma'^{-1} = \sigma''\sigma';$$

этим показана необходимость нашего условия. Обратно, пусть каждая пара инволюций, принадлежащих Ф, перестановочна. Тогда, если $\sigma_1, \ldots, \sigma_n$ — инволюции из Ф, то

$$(\sigma_1 \ldots \sigma_n)^2 = \sigma_1^2 \ldots \sigma_n^2 = 1;$$

отсюда следует, что каждый элемент подгруппы группы T, порожденной множеством Ф, будет инволюцией, т. е. эта подгруппа является группой инволюций.

Пусть теперь F-пространство A представлено в виде прямой суммы точек; множество всех точек, являющихся прямыми слагае-

мыми в этом разложении, обозначим через D. Наше предположение эквивалентно тому, что A является суммой точек из D и ни одна из точек, принадлежащих D, не лежит на гиперплоскости, порожденной остальными точками из D. Обозначим через $\Theta(D)$ *совокупность таких инволюций* σ, *что* $P\sigma = P$ *для каждой точки* P *из* D. Мы будем также говорить, что D является разложением F-пространства A в прямую сумму точек, а $\Theta(D)$ — системой инволюций, соответствующей разложению D.

Предложение 1. *Если* D *есть разложение* F*-пространства* A *в прямую сумму точек, то* $\Theta(D)$ *является максимальной группой инволюций.*

Доказательство. Если P — точка из D и если $P = Fp$, то для каждого σ из $\Theta(D)$ в теле F существует такое число e, что $p\sigma = ep$. Но σ является инволюцией; следовательно,

$$p = p\sigma^2 = e^2 p.$$

Тем самым показано, что $e = \pm 1$. Таким образом, если σ', σ'' — две произвольные инволюции из $\Theta(D)$, то $p\sigma' = \pm p$ и $p\sigma'' = \pm p$; отсюда следует, что $p\sigma'\sigma'' = p\sigma''\sigma'$ для любого элемента p, принадлежащего точке P. Так как это свойство справедливо для каждой точки P из D и A является суммой точек P, принадлежащих D, то любые две инволюции из $\Theta(D)$ перестановочны. Поэтому произведение инволюций, принадлежащих $\Theta(D)$, будет инволюцией. Отсюда ясно, что $\Theta(D)$ есть группа инволюций.

Пусть теперь Θ' — такая группа инволюций, что $\Theta(D) \leqslant \Theta'$. Если инволюция σ' принадлежит Θ', то, по лемме 1, $\sigma\sigma' = \sigma'\sigma$ для каждой инволюции σ из $\Theta(D)$. Отсюда и из предложения 1 (§ 2) следует, что

$$J^+(\sigma)\,\sigma' = J^+(\sigma) \text{ и } J^-(\sigma)\,\sigma' = J^-(\sigma) \text{ для каждого } \sigma \text{ из } \Theta(D).$$

Далее, если P — произвольная точка из D и P' — гиперплоскость, порожденная остальными точками, принадлежащими D, то $A = P \dotplus P'$; следовательно, существует, и притом только одна, такая инволюция σ, что $P = J^+(\sigma)$ и $P' = J^-(\sigma)$. Очевидно, что σ содержится в $\Theta(D)$; отсюда и из предыдущего замечания вытекает, что

$$P\sigma' = J^+(\sigma)\,\sigma' = J^+(\sigma) = P.$$

Таким образом, $P\sigma' = P$ для каждой точки P из D, и, следовательно, σ' принадлежит $\Theta(D)$. Этим показано, что $\Theta' = \Theta(D)$; т. е. $\Theta(D)$ является максимальной группой инволюций.

Предложение 2. *Следующие свойства максимальной группы* Θ *инволюций эквивалентны:*

(I) Θ *является системой инволюций, соответствующей разложению* D F*-пространства* A *в прямую сумму точек, т. е.* $\Theta = \Theta(D)$.

(II) *Если x — элемент из A, то множество $x\Theta$ (т. е. множество образов элемента x при всех инволюциях из Θ) порождает подпространство конечного ранга.*

(III) *A является суммой таких точек P, что $P = P\Theta$.*

(IV) *Если S — такое подпространство F-пространства A, что $\Theta \leqslant N\Delta(S)$, то Θ и $\Delta(S)^+$ имеют одну (и только одну) общую инволюцию.*

Доказательство. Пусть $\Theta = \Theta(D)$ для некоторого разложения D F-пространства A в прямую сумму точек. Если x – элемент из A, то существует такое конечное множество точек P_i из D, что x принадлежит подпространству $\sum_{i=1}^{n} P_i$. Поэтому в каждой точке P_i существует такой элемент p_i, что $x = \sum_{i=1}^{n} p_i$. Произвольная инволюция σ из Θ удовлетворяет условию $P_i\sigma = P_i$; поэтому $p_i\sigma$ принадлежит P_i и, следовательно, $x\sigma = \sum_{i=1}^{n} (p_i\sigma)$ принадлежит $\sum_{i=1}^{n} P_i$. Таким образом, множество $x\Theta$ является частью подпространства $\sum_{i=1}^{n} P_i$ конечного ранга n; этим показано, что из свойства (I) следует свойство (II).

Предположим теперь, что справедливо свойство (II), и обозначим через S сумму всех точек P, удовлетворяющих условию $P = P\Theta$ (мы будем такие точки называть Θ-инвариантными). Докажем прежде всего, что

(III*) *каждое Θ-инвариантное подпространство M, имеющее конечный ранг, содержится в S.*

Действительно, наше утверждение справедливо, очевидно, для точек. Поэтому можно предположить, что $r(M) > 1$; по индукции же предположим, что все Θ-инвариантные подпространства, ранги которых меньше $r(M)$, содержатся в S. Если инволюция σ принадлежит Θ, то $M\sigma = M$ и, следовательно, подпространство M вместе с элементом x содержит элементы $(x + x\sigma)/2$ и $(x - x\sigma)/2$. Так как x является суммой элементов $(x + x\sigma)/2$ и $(x - x\sigma)/2$ и один из этих элементов принадлежит $J^+(\sigma) \cap M$, а другой $J^-(\sigma) \cap M$, то

$$M = [J^+(\sigma) \cap M] \dotplus [J^-(\sigma) \cap M] \text{ для каждой инволюции } \sigma \text{ из } \Theta.$$

Рассмотрим два случая.

Случай 1: в Θ существует такая инволюция σ, что

$$0 < J^+(\sigma) \cap M < M.$$

Так как, по лемме 1, группа инволюций Θ коммутативна, то из предложения 1 (§ 2) следует, что $J^+(\sigma)$ и $J^-(\sigma)$ являются Θ-инвариантными подпространствами F-пространства A. Пересечение Θ-инвариантных подпространств будет, очевидно, Θ-инвариантным подпространством. Таким образом, мы представили M в виде прямой суммы двух Θ-инвариантных подпространств $M\bigcap J^+(\sigma)$ и $M\bigcap J^-(\sigma)$. Так как ранг первого слагаемого отличен от 0 и меньше $r(M)$, то то же самое справедливо и для второго слагаемого; отсюда и из индуктивного предположения вытекает, что $M\bigcap J^+(\sigma)$ и $M\bigcap J^-(\sigma)$ содержатся в S, а поэтому и M содержится в S.

Случай 2. В Θ не существует такой инволюции σ, что

$$0 < M\bigcap J^+(\sigma) < M.$$

В этом случае для каждой инволюции σ из Θ либо $M = M\bigcap J^+(\sigma) \leqslant J^+(\sigma)$, либо $M\bigcap J^+(\sigma) = 0$. Но так как M является прямой суммой подпространств $M\bigcap J^+(\sigma)$ и $M\bigcap J^-(\sigma)$, то из $M\bigcap J^+(\sigma) = 0$ следует, что $M = M\bigcap J^-(\sigma) \leqslant J^-(\sigma)$. Таким образом, для каждой инволюции σ из Θ либо $M \leqslant J^+(\sigma)$, либо $M \leqslant J^-(\sigma)$; но это означает, что каждое подпространство, содержащееся в M, является Θ-инвариантным. Отсюда, в частности, вытекает, что каждая точка, содержащаяся в M, является Θ-инвариантной и поэтому принадлежит S; следовательно, и само M содержится в S. Таким образом, методом индукции утверждение (III*) полностью доказано.

Пусть теперь x — произвольный элемент F-пространства A. Обозначим через X подпространство, порожденное x и всеми его образами $x\sigma$, где $\sigma \in \Theta$. Очевидно, что X будет Θ-инвариантным подпространством F-пространства A; в силу свойства (II), ранг $r(X)$ конечен. Отсюда и из утверждения (III*) вытекает, что X является частью подпространства S и, следовательно, S содержит x. Таким образом, $S = A$, и этим показано, что при выполнении свойства (II) выполняется и свойство (III).

Если справедливо свойство (III), то A будет суммой всех Θ-инвариантных точек. Поэтому существует такое множество D' Θ-инвариантных точек, что A разлагается в прямую сумму этих точек. Образуем группу инволюций $\Theta(D')$, соответствующую разложению D' F-пространства A в прямую сумму точек. По построению, каждая инволюция, принадлежащая Θ, оставляет инвариантной каждую точку из D'. Следовательно, $\Theta \leqslant \Theta(D')$. Но, по условию, Θ является максимальной группой инволюций, а $\Theta(D')$ является максимальной группой инволюций в силу предложения 1. Поэтому $\Theta = \Theta(D')$; этим показано, что из свойства (III) следует свойство (I). Таким образом, мы убедились в эквивалентности первых трех свойств. (В качестве полезного упражнения мы можем предложить читателю доказать, что $D = D'$.)

Пусть снова $\Theta = \Theta(D)$ для некоторого разложения D F-про-

странства A в прямую сумму точек, и пусть S — такое подпространство, что $\Theta \leqslant N\Delta(S)$. Тогда, если σ - инволюция из Θ, то, в силу предложения 1 (в) (§ 4), в $\Delta(S)^+$ существует такая инволюция τ, что $\tau\sigma = \sigma\tau$. Так как $S = J^+(\tau)$, то, используя предложение 1 (§ 2), мы получаем, что $S\sigma = S$. Таким образом, S является Θ-инвариантным подпространством и, следовательно (как было показано выше),

$$S = [J^+(\sigma) \cap S] \dotplus [J^-(\sigma) \cap S] \text{ для каждой инволюции } \sigma \text{ из } \Theta.$$

Если P — произвольная точка из D, то обозначим через P' гиперплоскость, порожденную остальными точками, принадлежащими D. Существует, и притом только одна, такая инволюция σ из $\Theta(D)$, что $P = J^+(\sigma)$, $P' = J^-(\sigma)$; это показывает, что либо $P \leqslant S$, либо $S \leqslant P'$ (для каждой точки P из D). Обозначим теперь через D_s совокупность точек P из D, содержащихся в S, а через D_s' — совокупность остальных точек, принадлежащих D. Тогда, если U — сумма точек из D_s, а V — пересечение всех гиперплоскостей P', являющихся дополнениями к точкам P из D_s', то $U \leqslant S \leqslant V$. Но так как A разлагается в прямую сумму точек из D, то $U = V$. Таким образом, показано, что S *является прямой суммой точек, принадлежащих* D_s.

Обозначим теперь через S' прямую сумму точек, принадлежащих D_s'. Очевидно, что $A = S \dotplus S'$; следовательно, существует, и притом только одна, такая инволюция ν, что $S = J^+(\nu)$, $S' = J^-(\nu)$. Так как каждая точка из D содержится либо в S, либо в S', то она инвариантна относительно ν. Таким образом, ν принадлежит пересечению систем Θ и $\Delta(S)^+$. (Различными способами можно проверить, что ν является единственной общей инволюцией указанных систем; проверку этого мы оставляем читателю.) Тем самым показано, что из свойства (I) следует свойство (IV).

Предположим, наконец, что выполняется свойство (IV). В таком случае справедливы следующие утверждения.

(IV.a) Если S является Θ-инвариантным подпространством F-пространства A, то в Θ найдется такая единственная инволюция τ, что $S = J^+(\tau)$; кроме того, в A существует одно и только одно такое Θ-инвариантное подпространство S', что $A = S \dotplus S'$.

Действительно, если σ — инволюция из Θ, то $\sigma^{-1}\Delta(S)^+\sigma = \Delta(S\sigma)^+ = \Delta(S)^+$, так что σ принадлежит $N\Delta(S)^+$. Таким образом, $\Theta \leqslant N\Delta(S)$; отсюда, в силу свойства (IV), следует существование инволюции τ, принадлежащей $\Theta \cap \Delta(S)^+$. Инволюция τ содержится в Θ и удовлетворяет условию $S = J^+(\tau)$. Так как τ перестановочна с каждой инволюцией σ из Θ, то, в силу предложения 1 (§ 2), подпространство $J^-(\tau) = S'$ будет Θ-инвариантным. Таким образом, мы нашли такое Θ-инвариантное подпространство S', что $A = S \dotplus S'$.

Предположим теперь, что существует второе Θ-инвариантное подпространство S'', являющееся дополнением S в A. Тогда, если x — элемент из S'', то $x\tau$, а следовательно, и $x+x\tau$ также принадлежат S''. В то же время элемент $x+x\tau$ принадлежит $J^+(\tau)=S$. Так как пересечение подпространства S и S'' равно 0, то $x+x\tau=0$. Но это означает, что x принадлежит $J^-(\tau)=S'$; тем самым показано, что $S''\leqslant S'$. Отсюда и из равенства $S\dotplus S'=S\dotplus S''$ следует, что $S'=S''$. Если τ' — другая инволюция из Θ, для которой $S=J^+(\tau')$, то $A=S\dotplus J^-(\tau')$ и подпространство $J^-(\tau')$ является Θ-инвариантным. Отсюда, как показано выше, вытекает, что $J^-(\tau')=J^-(\tau)$ и, следовательно, $\tau=\tau'$. Таким образом, утверждение (IV.а) полностью доказано.

(IV.б) Если подпространство S Θ-инвариантно и

(*) либо $S\leqslant J^+(\sigma)$, либо $S\leqslant J^-(\sigma)$ для всех σ из Θ,

то $r(S)\leqslant 1$.

В самом деле, допустим, вопреки утверждению, что $r(S)>1$. Тогда $S=U\dotplus V$, причем каждое из подпространств U и V отлично от 0 и S. В силу утверждения (IV.а), существует такое однозначно определенное Θ-инвариантное подпространство S', что $A=S\dotplus S'$. Существует, и притом только одна, такая инволюция ω, что $J^+(\omega)=S'\dotplus U$ и $J^-(\omega)=V$. Очевидно, что на подпространстве S' инволюция ω перестановочна с каждой инволюцией σ из Θ; в силу свойства (*), то же самое имеет место и на подпространстве S. Отсюда следует, что ω перестановочна с каждой инволюцией σ из Θ; используя теперь лемму 1 и максимальность группы Θ, мы получаем, что ω принадлежит Θ. Но это противоречит свойству (*), ибо оба подпространства U и V отличны от 0. Таким образом, $r(S)\leqslant 1$, что и требовалось доказать.

(IV.в). Каждое ненулевое Θ-инвариантное подпространство S F-пространства A содержит Θ-инвариантную точку.

Действительно, в S существует элемент $v\neq 0$. Обозначим через V подпространство, порожденное множеством $v\Theta$. Так как Θ является группой, то подпространство V Θ-инвариантно, причем V есть наименьшее Θ-инвариантное подпространство, содержащее v. Заметим теперь, что объединение упорядоченного (по включению) множества Θ-инвариантных подпространств является Θ-инвариантным подпространством. Отсюда и из теоретико-множественного принципа максимального элемента (см. добавление M) следует существование максимального Θ-инвариантного подпространства M, содержащегося в V и не содержащего элемент $v\neq 0$. В силу утверждения (IV.а), в A существует одно и только одно такое Θ-инвариантное подпространство M', что $A=M\dotplus M'$. Так как $M<V$, то $V=M\dotplus(M'\cap V)$, причем $M'\cap V\neq 0$.

Пусть $V'' = M' \cap V$. Подпространство V'', будучи пересечением двух Θ-инвариантных подпространств M' и V, Θ-инвариантно. Поэтому, если σ — инволюция из Θ, то, как мы не раз показывали, $V'' = [V'' \cap J^+(\sigma)] \dotplus [V'' \cap J^-(\sigma)]$ и оба подпространства $V'' \cap J^+(\sigma)$, $V'' \cap J^-(\sigma)$ Θ-инвариантны. Так как $V'' \neq 0$, то по крайней мере одна из компонент указанного прямого разложения отлична от 0. Пусть, например, $V'' \cap J^+(\sigma) \neq 0$. Тогда $M < M \dotplus [V'' \cap J^+(\sigma)] \leqslant V$. Теперь, воспользовавшись тем, что M является максимальным Θ-инвариантным подпространством, содержащимся в V и не содержащим v, а $V'' \cap J^+(\sigma)$ является Θ-инвариантным подпространством, мы получаем, что подпространство $M \dotplus [V'' \cap J^+(\sigma)]$ Θ-инвариантно, содержится в V и содержит элемент v. Но V является наименьшим Θ-инвариантным подпространством, содержащим v. Поэтому $M \dotplus V'' = V = M \dotplus [V'' \cap J^+(\sigma)]$ и, следовательно, $V'' = V'' \cap J^+(\sigma)$, т. е. $V'' \leqslant J^+(\sigma)$. Если отлично от 0 подпространство $V'' \cap J^-(\sigma)$, то подобным же образом можно убедиться, что $V'' \leqslant J^-(\sigma)$. Тем самым показано, что Θ-инвариантное подпространство $V'' \neq 0$, содержащееся в V, а поэтому и в S, удовлетворяет условию (*) утверждения (IV.б), из которого следует, что $r(V'') = 1$. Этим утверждение (IV.в) доказано.

Обозначим теперь через B сумму всех Θ-инвариантных точек F-пространства A. Подпространство B само Θ-инвариантно; поэтому, согласно утверждению (IV.а), существует такое Θ-инвариантное подпространство B', что $A = B \dotplus B'$. Если бы B' было отлично от 0, то в нем, в силу утверждения (IV.в), содержалась бы Θ-инвариантная точка, что невозможно, поскольку все Θ-инвариантные точки содержатся в B. Таким образом, $B' = 0$, и, следовательно, $A = B$, т. е. A представимо в виде суммы всех Θ-инвариантных точек. Этим показано, что при выполнении свойства (IV) выполняется и свойство (III), чем полностью доказана эквивалентность свойств (I) — (IV).

Из следующего предложения видно, что максимальная группа инволюций не всегда обладает указанными четырьмя эквивалентными свойствами (I) – (IV).

Предложение 3. *Следующие свойства линейного многообразия* (F, A) *эквивалентны.*

(I) *Ранг* $r(A)$ *конечен.*

(II) *Каждая максимальная группа инволюций соответствует некоторому разложению F-пространства A в прямую сумму точек.*

(III) *Любые две максимальные группы инволюций сопряжены в группе* $\mathrm{T}(F, A)$.

Доказательство. Если ранг $r(A)$ конечен, то каждая максимальная группа инволюций обладает свойством (II) предло-

жения 2 и поэтому соответствует некоторому разложению F-пространства A в прямую сумму точек. Таким образом, из свойства (I) следует свойство (II).

Пусть теперь справедливо свойство (II). Если D и D' — два разложения F-пространства A в прямую сумму точек, то, в силу теоремы единственности (гл. II, § 2), D и D' состоят из одного и того же числа $r(A)$ точек. Поэтому легко построить линейное преобразование σ, отображающее D на D' и, следовательно, удовлетворяющее условию $\sigma^{-1}\Theta(D)\sigma = \Theta(D')$. Этим показано, что при выполнении свойства (II) выполняется и свойство (III).

Пусть теперь справедливо свойство (III), и пусть Θ — произвольная максимальная группа инволюций. Пусть, далее, D — некоторое разложение F-пространства A в прямую сумму точек. Тогда, в силу свойства (III) и предложения 1, группы инволюций Θ и $\Theta(D)$ сопряжены. Следовательно, существует такое линейное преобразование σ, что

$$\Theta = \sigma^{-1}\Theta(D)\sigma = \Theta(D\sigma);$$

тем самым показано, что свойство (II) вытекает из свойства (III).

Предположим, наконец, что ранг $r(A)$ бесконечен. Тогда $A = U + V$, где U — подпространство, обладающее счетным базисом $b_1, b_2, \ldots, b_i, \ldots$. Так как U можно также представить в виде прямой суммы точек $F(b_1 - b_2), \ldots, F(b_i - b_{i+1}), Fb_{i+1}, \ldots, Fb_{i+j}, \ldots$, то существует, и притом только одна, такая инволюция σ_i, что

$$J^+(\sigma_i) = \sum_{j=1}^{i} F(b_j - b_{j+1}), \qquad J^-(\sigma_i) = V + \sum_{j>i} Fb_j.$$

Из предложения 1 (§ 2) следует, что $\sigma_i\sigma_k = \sigma_k\sigma_i$ для любых i и k. Отсюда и из леммы 1 вытекает, что инволюции σ_i принадлежат некоторой группе инволюций; применяя теперь теоретико-множественный принцип максимального элемента, мы можем найти максимальную группу Θ инволюций, содержащую все инволюции σ_i. Но

$$b_1\sigma_i = \left[\sum_{j=1}^{i}(b_j - b_{j+1}) + b_{i+1}\right]\sigma_i = b_1 - 2b_{i+1};$$

следовательно, $b_1\Theta$ содержит счетное множество линейно независимых элементов $b_1 - 2b_2, b_1 - 2b_3, \ldots, b_1 - 2b_{i+1}, \ldots$. Таким образом, группа Θ инволюций не обладает свойством (II) предложения 2 и поэтому не соответствует никакому разложению F-пространства A в прямую сумму точек. Этим показано, что если ранг $r(A)$ бесконечен, то F-пространство A не обладает свойством (II). Тем самым мы убедились, что свойство (I)

является следствием свойства II, и этим завершается доказательство предложения.

Замечание 1. Если D — разложение F-пространства A в прямую сумму точек, то нетрудно проверить, что точка P тогда и только тогда принадлежит D, когда она $\Theta(D)$-инвариантна. Это показывает, что отображение Θ определяет взаимно однозначное соответствие между всеми разложениями F-пространства A в прямую сумму точек и всеми максимальными группами инволюций, в которых выполняются свойства (I) – (IV) предложения 2.

Замечание 2. Если D есть разложение F-пространства A в прямую сумму точек, то $\Theta(D)$ состоит точно из $2^{r(A)}$ инволюций, ибо каждому подмножеству точек из D можно сопоставить одну и только одну инволюцию из $\Theta(D)$, оставляющую неподвижными все элементы каждой точки данного подмножества. Поэтому, если ранг $r(A)$ конечен, то он полностью определяется порядком максимальной группы инволюций; в случае же бесконечности ранга $r(A)$ соответствующая задача оказывается связанной с так называемой проблемой континуума.

§ 6. Характеристика полной линейной группы как подгруппы группы полулинейных преобразований

В § 2 гл. III мы уже отмечали, что полная линейная группа $\mathrm{T}(F, A)$ линейного многообразия (F, A) является нормальным делителем группы $\Lambda(F, A)$ всех полулинейных преобразований F-пространства A. В настоящем параграфе мы усилим этот результат и покажем, что T является подгруппой группы Λ, инвариантной при изоморфных отображениях этой группы на любую другую группу полулинейных преобразований. Это нам позволит, опираясь на результаты первой части настоящей главы, получить в следующем § 7 результаты, относящиеся к изоморфизмам группы Λ, аналогичные тем, которые в § 5 мы получили для группы T.

В этом и в следующем параграфах мы будем предполагать, что рассматриваемые линейные многообразия имеют *характеристику, отличную от 2, и ранг, не меньший 3*, хотя некоторые из результатов, которые мы здесь получим, остаются справедливыми и без указанных предположений.

Напомним, что каждое полулинейное преобразование σ линейного многообразия (F, A) на себя представляет собой пару, состоящую из автоморфизма σ тела F и автоморфизма σ аддитивной группы A, связанных между собой следующим соотношением: $(f a)^{\sigma} = f^{\sigma} a^{\sigma}$ для f из F и a из A. Первый из этих автоморфизмов нам удобно называть F-компонентой полулинейного преобразования σ. (Заметим, что мы снова возвращаемся к показательной записи действия преобразования.)

Лемма 1. *Полулинейное преобразование σ тогда и только тогда будет инволюторным, но не линейным, когда*

(а) *в F-пространстве A существует базис, каждый элемент которого остается неподвижным относительно σ;*

(б) *E-компонента полулинейного преобразования σ является инволюторным автоморфизмом, отличным от тождественного.*

Доказательство. Достаточность наших условий очевидна. Предположим теперь, что $\sigma^2 = 1$ и что σ не является линейным преобразованием. Тогда необходимость условия (б) почти непосредственно следует из того, что полулинейное преобразование тогда и только тогда будет линейным, когда его F-компонента является тождественным автоморфизмом. Поскольку характеристика тела F отлична от 2, каждый элемент a из A и каждый элемент f из F можно представить в виде:

$$a = \frac{1}{2}(a + a^\sigma) + \frac{1}{2}(a - a^\sigma), \quad f = \frac{1}{2}(f + f^\sigma) + \frac{1}{2}(f - f^\sigma);$$

первые слагаемые в этих суммах являются σ-неподвижными, а вторые меняют при σ знаки. Отсюда видно, что так как F-компонента отлична от 1, то в F существует такой элемент $i \neq 0$, что $i^\sigma = -i$. Если теперь a является σ-неподвижным элементом F-пространства A, то $(ia)^\sigma = i^\sigma a^\sigma = -ia$, так что элемент ia меняет при σ знак. Поэтому каждый элемент x из A можно представить в виде $x = x' + ix''$, где x' и x'' — оба σ-неподвижные элементы $[x' = (x + x^\sigma)/2$ и $x'' = i^{-1}(x - x^\sigma)/2]$. Отсюда непосредственно следует существование в F-пространстве A базиса, состоящего лишь из σ-неподвижных элементов, что и доказывает необходимость условия (а).

Лемма 2. *Инволюторные полулинейные преобразования, не являющиеся линейными, тогда и только тогда сопряжены в группе Λ, когда сопряжены их F-компоненты (в группе всех автоморфизмов тела F).*

Доказательство. Необходимость нашего условия непосредственно следует из того, что умножение полулинейных преобразований происходит покомпонентно (так что, в частности, произведение полулинейных преобразований имеет F-компоненту, равную произведению F-компонент множителей). Пусть теперь σ' и σ'' — инволюторные полулинейные преобразования, причем ни σ', ни σ'' не являются линейными, и пусть существует такой автоморфизм α тела F, что для F-компонент полулинейных преобразований σ' и σ'' имеет место соотношение $\sigma'' = \alpha^{-1}\sigma'\alpha$. В силу леммы 1, в F-пространстве A существуют базис B', состоящий из σ'-неподвижных элементов, и базис B'', состоящий из σ''-неподвижных элементов. Так как B' и B'' содержат одно и то же число элементов [а именно $r(A)$], то существует взаимно однозначное отображение базиса B' на базис B''; следовательно,

существует полулинейное преобразование β, имеющее F-компоненту, равную α, отображающее базис B' на базис B''. Легко проверить, что F-компонента полулинейного преобразования $\beta^{-1}\sigma'\beta$ совпадает с F-компонентой полулинейного преобразования σ'' и что $\beta^{-1}\sigma'\beta$, так же как и σ'', оставляет неподвижным каждый элемент базиса B''. Отсюда $\sigma''=\beta^{-1}\sigma'\beta$, что и требовалось доказать.

Предложение 1. *Если σ — инволюторное полулинейное преобразование, то σ и $-\sigma$ [последнее преобразование имеет вид $(\sigma, -\sigma)$] тогда и только тогда являются сопряженными полулинейными преобразованиями, когда*

$$\text{либо } \sigma \text{ не линейно, либо } r[J^+(\sigma)]=r[J^-(\sigma)]. \quad (*)$$

Замечание 1. Если инволюторное полулинейное преобразование σ не является линейным, то из леммы 1 следует, что ни совокупность всех σ-неподвижных элементов из A, ни совокупность всех элементов, меняющих при σ знак, не являются подпространствами F-пространства A и что каждая из этих совокупностей порождает все A.

Доказательство. Предположим сначала, что σ является линейным преобразованием и что $-\sigma=\alpha^{-1}\sigma\alpha$, где α — некоторое полулинейное преобразование. Тогда

$$J^-(\sigma)=J^+(-\sigma)=J^+(\alpha^{-1}\sigma\alpha)=J^+(\sigma)^\alpha;$$

отсюда следует справедливость условия (*), ибо при полулинейном преобразовании сохраняется ранг (см. гл. III, § 1).

Обратно, пусть выполняется условие (*). Если σ не линейно, то σ и $-\sigma$ являются инволюторными полулинейными преобразованиями с одной и той же F-компонентой и ни σ, ни $-\sigma$ не являются линейными преобразованиями. Отсюда и из леммы 2 следует, что σ и $-\sigma$ сопряжены в Λ. Если же σ — линейное преобразование, то, по условию (*), $r[J^+(\sigma)]=r[J^-(\sigma)]$. Поскольку, кроме того, $A=J^+(\sigma)\dotplus J^-(\sigma)$, существует такая инволюция τ F-пространства A, при которой $J^+(\sigma)$ отображается на $J^-(\sigma)$, а $J^-(\sigma)$ на $J^+(\sigma)$. Поэтому

$$J^+(\sigma)=J^-(\sigma)^\tau=J^-(\tau\sigma\tau), \quad J^-(\sigma)=J^+(\sigma)^\tau=J^+(\tau\sigma\tau),$$

и, следовательно, $\tau\sigma\tau=-\sigma$. Этим предложение 1 полностью доказано.

Замечание 2. Заметим, что тогда и только тогда существует инволюторное линейное преобразование (т. е. инволюция), обладающее свойством (*), когда либо ранг $r(A)$ бесконечен, либо $r(A)$ — четное число.

Замечание 3. Если мы, как обычно, обозначим через -1 линейное преобразование F-пространства A, отображающее каждый элемент a из A на элемент $-a$, то полулинейное преобра-

зование $-\sigma$, о котором говорилось в предложении 1, можно представить в виде $-\sigma=(-1)\sigma$, и этим оправдывается принятое нами обозначение этого полулинейного преобразования через $-\sigma$. Заметим, что поскольку центр группы Λ является, очевидно, частью центра группы T, то, в силу предложения 2 (§ 1), линейное преобразование -1 однозначно определяется в группе Λ как *единственный элемент центра, имеющий порядок* 2.

Обозначим через N^* *множество всех инволюторных полулинейных преобразований* σ, *не сопряженных с* $-\sigma$. Из замечания 3 следует, что N^* является теоретико-групповым инвариантом группы Λ, и, в силу предложения 1, N^* содержится в T.

Напомним, что полулинейное преобразование σ называется *тривиальным*, если в теле F существует такое число $f\neq 0$, что $x^\sigma=fx$ для каждого x из A; F-компонентой этого полулинейного преобразования будет внутренний автоморфизм тела F, индуцированный элементом f. В гл. III, §§ 1 и 2, мы уже указывали, что совокупность N тривиальных полулинейных преобразований является нормальным делителем группы Λ.

Предложение 2. N *является централизатором множества* N^* *в группе* Λ.

Доказательство. Выше было указано, что, как следует из предложения 1, $N^*\leqslant T$. Поэтому централизатор подгруппы T в группе Λ будет частью централизатора множества N^* в Λ. Но при исследовании групп преобразований (гл. III, § 2) было показано, что T является централизатором нормального делителя N в группе Λ. Следовательно, каждый элемент из N перестановочен с каждым элементом из N^*; этим показано, что N содержится в централизаторе множества N^*.

Пусть теперь полулинейное преобразование σ перестановочно с каждым линейным преобразованием из N^*. Возьмем произвольную точку P F-пространства A. Существует такая инволюция ν, принадлежащая T, что $P=J^+(\nu)$. Так как $r(A)\geqslant 3$, то $1=r(P)<r[J^-(\nu)]$ и, в силу предложения 1, ν принадлежит N^*. Следовательно, $\nu\sigma=\sigma\nu$, и поэтому

$$P=J^+(\nu)=J^+(\sigma^{-1}\nu\sigma)=J^+(\nu)^\sigma=P^\sigma.$$

Таким образом, полулинейное преобразование σ индуцирует тождественное проективное отображение; отсюда и из предложения 3 (гл. III, § 1) вытекает, что σ является тривиальным полулинейным преобразованием, т. е. что оно принадлежит N. Этим показано, что N совпадает с централизатором множества N^* в группе Λ.

Теорема 1. *Полная линейная группа* T *является вторым централизатором множества* N^* *в группе* Λ.

Доказательство. Согласно предложению 2, N является централизатором множества N^* в группе Λ; в то же время, как

было показано при исследовании групп преобразований линейного многообразия (гл. III, § 2), T является централизатором нормального делителя N в группе Λ. Отсюда следует, что T представляет собой второй централизатор множества N* в группе Λ.

Теорема 2. *Каждое изоморфное отображение группы* $\Lambda(F, A)$ *на группу* $\Lambda(G, B)$ *отображает* $N^*(F, A)$, $N(F, A)$ *и* $T(F, A)$ *соответственно на* $N^*(G, B)$, $N(G, B)$ *и* $T(G, B)$.

Доказательство. Так как -1 является единственной нетождественной инволюцией, содержащейся в центре группы $\Lambda(F, A)$, то при любом изоморфном отображении σ группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$ элемент -1 [из $\Lambda(F, A)$] отображается на элемент -1 [из $\Lambda(G, B)$]. Отсюда и из определения множества N* следует, что σ отображает $N^*(F, A)$ на $N^*(G, B)$; используя теперь предложение 2 и теорему 1, мы легко убедимся, что σ отображает $N(F, A)$ на $N(G, B)$ и $T(F, A)$ на $T(G, B)$.

§ 7. Изоморфизмы группы полулинейных преобразований

Пусть (F, A) и (G, B) — линейные многообразия, характеристики которых отличны от 2 и ранги которых не меньше 3. Тогда имеет место следующая

Структурная теорема. *Группы* $\Lambda(F, A)$ *и* $\Lambda(G, B)$ *изоморфны тогда и только тогда, когда линейные многообразия* (F, A) *и* (G, B) *либо проективно эквивалентны, либо двойственны друг другу.*

Из этой теоремы и структурной теоремы § 5 следует, что группы $T(F, A)$ и $T(G, B)$ изоморфны тогда и только тогда, когда изоморфны группы $\Lambda(F, A)$ и $\Lambda(G, B)$.

Только что сформулированную структурную теорему мы получим в качестве следствия из теорем, в которых полностью описываются все изоморфные отображения (если они существуют) группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$. Мы начнем с перечисления некоторых классов таких изоморфных отображений. Они похожи на соответствующие изоморфные отображения группы $T(F, A)$, строившиеся нами в § 5, хотя и сложнее последних.

Сингулярные автоморфизмы группы $\Lambda(F, A)$. Автоморфизм α группы $\Lambda(F, A)$ называется *сингулярным*, если $\sigma^\alpha\sigma^{-1}$ принадлежит N для каждого полулинейного преобразования σ из Λ.

Каждое полулинейное преобразование σ, принадлежащее N, имеет вид $x^\sigma = fx$, где f — отличное от 0 фиксированное число из F; поэтому это полулинейное преобразование можно отождествить с соответствующим ему числом f; такое отождествление мы и будем делать. Если теперь σ — полулинейное преобразование, a — произвольный элемент F-пространства A и f — отличное от 0 число из F, то

$$a^{\sigma^{-1}f\sigma} = (fa^{\sigma^{-1}})^\sigma = f^\sigma a, \quad \text{откуда} \quad \sigma^{-1}f\sigma = f^\sigma. \qquad (1)$$

Если α — сингулярный автоморфизм группы Λ, то для каждого полулинейного преобразования σ из Λ положим $\sigma^* = \sigma^\alpha \sigma^{-1}$; легко видеть, что

$$(\sigma\tau)^* = \sigma^\alpha \tau^\alpha \tau^{-1}\sigma^{-1} = \sigma^\alpha_\sigma \sigma^{-1}\sigma\tau^\alpha\tau^{-1}\sigma^{-1} = \sigma^*\tau^{*\sigma^{-1}}. \quad (2)$$

Отображение σ в σ^* является, следовательно, так называемым *скрещенным гомоморфизмом группы Λ в ее подгруппу* N *или в мультипликативную группу тела* F. Легко проверить, что такой скрещенный гомоморфизм группы Λ в мультипликативную группу тела F тогда и только тогда задается некоторым сингулярным автоморфизмом группы Λ, когда отображение числа f из F в число f^*f является автоморфизмом мультипликативной группы тела F (напомним, что мы отождествили мультипликативную группу тела F с группой N).

Предложение 1. *Следующие свойства автоморфизма α группы Λ эквивалентны:*

(I) *α является сингулярным автоморфизмом группы Λ.*

(II) *α индуцирует сингулярный автоморфизм группы* T.

(III) $\Delta(S)^\alpha = \Delta(S)$ *для каждого подпространства S F-пространства A.*

Доказательство. Пусть α — сингулярный автоморфизм группы Λ. Из теоремы 2 (§ 6) следует, что α индуцирует автоморфизм группы T. Поэтому, если σ — линейное преобразование, то σ и σ^α оба принадлежат T. Следовательно, $\sigma^\alpha\sigma^{-1}$ содержится в пересечении подгрупп T и N. Но T является централизатором подгруппы N в группе Λ (см. исследование групп преобразований линейного многообразия, гл. III, § 2); поэтому пересечение подгрупп T и N совпадает с центром подгруппы N. В силу же предложения 2 (§ 1), центр подгруппы N совпадает с центром Z группы T; этим показано, что α индуцирует сингулярный автоморфизм группы T, т. е. свойство (II) следует из свойства (I).

Из предложения 1 (§ 5) непосредственно следует, что если выполняется свойство (II), то выполняется и свойство (III).

Пусть, наконец, справедливо свойство (III). Если σ — полулинейное преобразование из Λ, то положим $\sigma^* = \sigma^\alpha\sigma^{-1}$. Из свойства (III) следует, что

$$\Delta(S^{\sigma^*}) = \sigma^{*-1}\Delta(S)\sigma^* = \sigma\sigma^{-\alpha}\Delta(S)\sigma^\alpha\sigma^{-1} = \sigma[\sigma^{-1}\Delta(S)\sigma]^\alpha\sigma^{-1} =$$

$$= \sigma[\Delta(S^\sigma)]^\alpha\sigma^{-1} = \sigma\Delta(S^\sigma)\sigma^{-1} = \Delta(S)$$

для каждого подпространства S F-пространства A; отсюда и из теоремы 3 (б) (§ 4) вытекает, что $S^{\sigma^*} = S$ для каждого подпространства S F-пространства A. Но, в силу предложения 3 (гл. III, § 1), полулинейные преобразования, индуцирующие тождественное проективное отображение, принадлежат N; таким образом, σ^*

для каждого σ из Λ принадлежит N и, следовательно, α является сингулярным автоморфизмом группы Λ. Этим показано, что свойство (I) вытекает из свойства (III).

Предложение 1, в частности, показывает, что определение сингулярного автоморфизма, введенное в настоящем параграфе, полностью согласуется с определением сингулярного автоморфизма, данным в § 5.

Индуцированные изоморфизмы 1-го рода. Пусть σ — полулинейное преобразование линейного многообразия (F, A) на линейное многообразие (G, B). Тогда, если τ — полулинейное преобразование из $\Lambda(F, A)$, то $\sigma^{-1}\tau\sigma = \tau^{\sigma}$ будет полулинейным преобразованием из $\Lambda(G, B)$; отображение τ в τ^{σ} определяет изоморфное отображение группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$. Это изоморфное отображение группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$ мы будем называть *изоморфным отображением, индуцированным полулинейным преобразованием* σ [линейного многообразия (F, A) на линейное многообразие (G, B)], или *индуцированным изоморфным отображением первого рода.*

Индуцированные автоморфизмы первого рода совпадают с внутренними автоморфизмами группы $\Lambda(F, A)$. Элемент из $\Lambda(F, A)$ тогда и только тогда индуцирует тождественный автоморфизм, когда он принадлежит центру группы $\Lambda(F, A)$. Докажем теперь следующее простое утверждение.

Лемма 1. *Полулинейное преобразование σ тогда и только тогда принадлежит центру группы $\Lambda(F, A)$, когда оно имеет вид $x^{\sigma} = fx$, где f — отличный от 0 элемент из центра тела F, остающийся неподвижным при каждом автоморфизме тела F.*

Доказательство. Очевидно, что каждый элемент из центра группы Λ принадлежит централизатору множества N^* в Λ, которым является подгруппа N тривиальных полулинейных преобразований. Если f — отличное от 0 число из F и σ — полулинейное преобразование, то, по формуле (1), для тривиального полулинейного преобразования, определяемого числом f, имеет место соотношение $f^{\sigma} = \sigma^{-1}f\sigma$. Таким образом, это тривиальное полулинейное преобразование тогда и только тогда принадлежит центру группы Λ, когда $f^{\sigma} = f$ для каждого автоморфизма σ тела F [ибо каждый автоморфизм тела F входит в качестве F-компоненты по крайней мере в одно полулинейное преобразование из $\Lambda(F, A)$]. Отсюда непосредственно следует справедливость леммы 1.

Каждый автоморфизм группы Λ индуцирует автоморфизм группы T. Если z — элемент из центра Z группы T, то, в силу предложения 1 (§ 1), z можно рассматривать как элемент центра тела F. Таким образом, элементы, принадлежащие центру тела F, задают внутренние автоморфизмы группы Λ, индуцирующие тождественный автоморфизм на подгруппе T, хотя в общем

случае, как следует из леммы 1, такие автоморфизмы не являются тождественными на всей группе Λ.

Построение индуцированных изоморфных отображений второго рода несколько более сложно и очень близко к аналогичным построениям, которые мы проводили в гл. V, § 5. Начнем с построения *естественного инверсно изоморфного отображения и естественного изоморфного отображения группы* $\Lambda(F, A)$ *в группу* $\Lambda(A^*, F)$ [где (A^*, F) — пространство, сопряженное к линейному многообразию (F, A); см. гл. II, § 3].

Пусть σ — полулинейное преобразование из $\Lambda(F, A)$. Тогда для каждой линейной формы f над A определим следующим образом отображение f^{σ^*} аддитивной группы A в тело F:

$$af^{\sigma^*} = (a^\sigma f)^{\sigma^{-1}} \text{ для каждого } a \text{ из } A. \tag{3}$$

Очевидно, что отображение f^{σ^*} сохраняет сложение; так как

$$(xa)f^{\sigma^*} = [(xa)^\sigma f]^{\sigma^{-1}} = [x^\sigma (a^\sigma f)]^{\sigma^{-1}} = x(af^{\sigma^*}),$$

то f^{σ^*} является линейной формой над A. Отсюда ясно, что σ^* будет взаимно однозначным отображением аддитивной группы A^* в себя, сохраняющим сложение. Докажем теперь, что

$$(fy)^{\sigma^*} = f^{\sigma^*} y^{\sigma^{-1}} \text{ для } f \text{ из } A^* \text{ и } y \text{ из } F. \tag{3а}$$

Справедливость этого утверждения вытекает из того, что для каждого a из A

$$a(fy)^{\sigma^*} = [a^\sigma (fy)]^{\sigma^{-1}} = [(a^\sigma f)\, y]^{\sigma^{-1}} = (a^\sigma f)^{\sigma^{-1}} y^{\sigma^{-1}} = (af^{\sigma^*})y^{\sigma^{-1}} = a(f^{\sigma^*} y^{\sigma^{-1}}).$$

Далее докажем, что

$$(\sigma\tau)^* = \tau^*\sigma^* \text{ для любых } \sigma, \tau \text{ из } \Lambda(F, A). \tag{4}$$

Справедливость этого утверждения вытекает из того, что для каждого a из A и каждого f из A^*

$$af^{(\sigma\tau)^*} = (a^{\sigma\tau} f)^{\tau^{-1}\sigma^{-1}} = ([(a^\sigma)^\tau f]^{\tau^{-1}})^{\sigma^{-1}} = [a^\sigma f^{\tau^*}]^{\sigma^{-1}} = a(f^{\tau^*})^{\sigma^*} = af^{\tau^*\sigma^*}.$$

Так как $1^* = 1$, то, очевидно, каждое отображение σ^* обладает обратным, и, следовательно, σ^* является полулинейным преобразованием, принадлежащим группе $\Lambda(A^*, F)$; его F-компонента обратна F-компоненте полулинейного преобразования σ. Отображение σ в σ^* определяет, очевидно, *естественное инверсно изоморфное отображение группы* $\Lambda(F, A)$ *в группу* $\Lambda(A^*, F)$. Поскольку отображение каждого элемента группы на обратный к нему элемент является инверсным автоморфизмом группы, мы получим изоморфное отображение группы $\Lambda(F, A)$ в группу $\Lambda(A^*, F)$, если каждому полулинейному преобразованию σ из $\Lambda(F, A)$ сопоставим полулинейное преобразование σ^{*-1} из $\Lambda(A^*, F)$. Это

изоморфное отображение мы назовем *естественным изоморфным отображением группы* $\Lambda(F, A)$ *в группу* $\Lambda(A^*, F)$. [Заметим, что σ и σ^{*-1} имеют одну и ту же F-компоненту.]

Предложение 2. *Следующие свойства линейного многообразия* (F, A) *эквивалентны:*

(I) *При естественном изоморфном отображении группа* $\Lambda(F, A)$ *отображается на всю группу* $\Lambda(A^*, F)$.

(II) *Группы* $\Lambda(F, A)$ *и* $\Lambda(A^*, F)$ *изоморфны.*

(III) *Ранг* $r(A)$ *конечен.*

Доказательство. Очевидно, что из свойства (I) следует свойство (II). Пусть теперь справедливо свойство (II). Тогда, в силу теоремы 2 (§ 6), группы $T(F, A)$ и $T(A^*, F)$ также будут изоморфны. Но в таком случае, как следует из структурной теоремы (§ 5), линейные многообразия (F, A) и (A^*, F) либо проективно эквивалентны, либо двойственны друг другу (читатель может проверить, что это утверждение не перестает быть верным от того, что элементы из A умножаются на числа из F слева, а элементы из A^* — справа). В обоих случаях имеет место равенство $r(A) = r(A^*)$, из которого, в силу следствия 1 (гл. II, § 3), вытекает, что ранг $r(A)$ конечен. Таким образом, если справедливо свойство (II), то справедливо и свойство (III).

Допустим, наконец, что ранг $r(A)$ конечен. Для того, чтобы доказать, что в этом случае выполняется свойство (I), достаточно показать, что при естественном инверсно изоморфном отображении группа $\Lambda(F, A)$ отображается на всю группу $\Lambda(A^*, F)$; это мы сейчас и сделаем. Пусть τ — произвольное полулинейное преобразование из $\Lambda(A^*, F)$. Если a — элемент F-пространства A, то определим следующим образом однозначное отображение a' аддитивной группы A^* в тело F:

$$a'f = (af^{\tau})^{\tau^{-1}} \text{ для каждого } f \text{ из } A^*. \qquad (3^*)$$

Прямым подсчетом нетрудно проверить, что a' является линейной формой над (A^*, F). Так как ранг $r(A)$ конечен, то, согласно теореме 2 (гл. II, § 3), существует один и только один такой элемент a^{σ} из A, что $a^{\sigma}f = a'f$ для каждого f из A^*. Таким образом, мы можем каждому полулинейному преобразованию τ из $\Lambda(A^*, F)$ сопоставить определенное однозначное отображение $\sigma = \sigma(\tau)$ аддитивной группы A в себя. Это отображение, по самому его определению, обладает следующим свойством, вытекающим из соотношения (3*):

$$a^{\sigma(\tau)}f = (af^{\tau})^{\tau^{-1}} \text{ для каждого } a \text{ из } A \text{ и каждого } f \text{ из } A^*. \quad (3^+)$$

Подобно тому, как это было проведено выше, легко проверить, что

$$(xa)^{\sigma(\tau)} = x^{\tau^{-1}} a^{\sigma(\tau)} \text{ для } x \text{ из } F \text{ и } a \text{ из } A,$$

$$\sigma(\tau'\tau'') = \sigma(\tau'')\,\sigma(\tau'), \quad \sigma(1) = 1;$$

отсюда, в частности, следует, что $\sigma(\tau)$ является полулинейным преобразованием из $\Lambda(F, A)$, F-компонента которого равна τ^{-1}. Используя теперь определение (3) естественного инверсно изоморфного отображения группы $\Lambda(F, A)$ в группу $\Lambda(A^*, F)$, мы получаем

$$af^{\sigma(\tau)^*} = (a^{\sigma(\tau)}f)^{\sigma(\tau)^{-1}} = (a^{\sigma(\tau)}f)^{\tau} = [(af^{\tau})^{\tau^{-1}}]^{\tau} = af^{\tau}$$

для каждого a из A и каждого f из A^*. Но если две линейные формы над A принимают одинаковые значения для каждого a из A, то они совпадают. Таким образом, $f^{\tau} = f^{\sigma(\tau)^*}$ для каждого f из A^* и, следовательно, $\tau = \sigma(\tau)^*$, т. е. τ является образом полулинейного преобразования $\sigma(\tau)$ при естественном инверсно изоморфном отображении группы $\Lambda(F, A)$ в группу $\Lambda(A^*, F)$. Отсюда следует, что

$$[\Lambda(F, A)]^* = \Lambda(A^*, F);$$

этим показано, что при выполнении свойства (III) выполняется и свойство (I), чем и завершается доказательство предложения 2.

Замечание 1. Если ранг $r(A)$ конечен, то, по теореме 2 (гл. II, § 3), A является пространством, сопряженным к линейному многообразию (A^*, F), и в этом случае отображение $\sigma(\tau)$ по существу совпадает с естественным инверсно изоморфным отображением группы $\Lambda(A^*, F)$ в группу $\Lambda(F, A)$.

Теперь мы можем построить

Индуцированные изоморфизмы 2-го рода. Рассмотрим произвольное инверсно полулинейное преобразование σ сопряженного пространства (A^*, F) на линейное многообразие (G, B). Если α есть полулинейное преобразование из $\Lambda(A^*, F)$, то $\sigma^{-1}\alpha\sigma = \alpha^{\sigma}$, как легко видеть, будет полулинейным преобразованием из $\Lambda(G, B)$; при доказательстве этого утверждения нужно принять во внимание, что если σ есть инверсно изоморфное отображение тела F на тело G и α — автоморфизм тела F, то $\sigma^{-1}\alpha\sigma$ будет автоморфизмом тела G. Очевидно, что отображение α на α^{σ} определяет изоморфное отображение группы $\Lambda(A^*, F)$ на группу $\Lambda(G, B)$. Обозначим теперь через $\cdot^{\nu}$ естественное изоморфное отображение группы $\Lambda(F, A)$ в группу $\Lambda(A^*, F)$, так что $\tau^{\nu} = \tau^{*-1}$ для каждого τ из $\Lambda(F, A)$. Тогда $\nu\sigma$ будет изоморфным отображением группы $\Lambda(F, A)$ в группу $\Lambda(G, B)$; $\nu\sigma$ мы будем называть *изоморфным отображением, индуцированным инверсно полулинейным преобразованием* σ, или *индуцированным изоморфным отображением второго рода*.

Так как отображение элемента α из $\Lambda(A^*, F)$ на элемент α^{σ} из $\Lambda(G, B)$ определяет изоморфное отображение группы $\Lambda(A^*, F)$ на группу $\Lambda(G, B)$, то $\nu\sigma$ тогда и только тогда будет изоморфным отображением группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$, когда ν

будет изоморфным отображением группы $\Lambda(F, A)$ на группу $\Lambda(A^*, F)$. Последнее условие, в силу предложения 2, эквивалентно конечности ранга $r(A)$. Полученный результат можно сформулировать в виде следующего утверждения.

Следствие 1. *Индуцированные изоморфные отображения второго рода тогда и только тогда являются «изоморфными отображениями на», когда ранг исходного линейного многообразия конечен.*

Замечание 2. Так как всегда существуют инверсно полулинейные преобразования сопряженного пространства (A^*, F) (см., например, гл. IV, § 1, построение канонического двойственного пространства), то всегда существуют индуцированные изоморфные отображения второго рода. Отсюда видно, что из существования изоморфного отображения второго рода группы $\Lambda(F, A)$ в группу $\Lambda(G, B)$ автоматически не следует, что оно будет изоморфным отображением группы $\Lambda(F, A)$ на всю группу $\Lambda(G, B)$; этим объясняется необходимость введения дополнительного предположения о конечности ранга.

Замечание 3. Читатель может сам убедиться в справедливости следующего утверждения. Если изоморфное отображение σ группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$ является индуцированным изоморфным отображением первого (второго) рода, то изоморфное отображение группы $\mathrm{T}(F, A)$ на группу $\mathrm{T}(G, B)$, определяемое σ, будет индуцированным изоморфным отображением первого (второго) рода в смысле § 5.

Мы теперь подготовлены к тому, чтобы сформулировать следующий основной результат.

Теорема об изоморфном отображении. *Каждое изоморфное отображение группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$ можно представить, и притом по существу однозначно, в виде $\sigma'\sigma''$, где σ' — сингулярный автоморфизм группы $\Lambda(F, A)$ и σ'' — индуцированное изоморфное отображение (первого или второго рода) группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$.*

Здесь мы говорим, что два представления $\sigma = \sigma'\sigma'' = \tau'\tau''$ изоморфного отображения σ в виде произведений сингулярных автоморфизмов σ', τ' и индуцированных изоморфных отображений σ'', τ'' *по существу совпадают*, если σ'' и τ'' являются индуцированными изоморфными отображениями одного и того же рода и $\tau'^{-1}\sigma' = \tau''\sigma''^{-1}$ есть внутренний автоморфизм, индуцированный элементом из N (т. е. индуцированный тривиальным полулинейным преобразованием).

Доказательству этой основной теоремы мы предпошлем доказательство нескольких утверждений.

Предложение 3. *Если σ — изоморфное отображение группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$, то существует такое однозначно определенное проективное или дуальное отображение σ'*

F-пространства A на G-пространство B, что

$$\Delta(S^{\sigma'}) = \Delta(S)^{\sigma} \text{ и } S^{\sigma'} = J^{+}([\Delta(S)^{2}]^{\sigma})$$

для каждого отличного от 0 *и A подпространства S F-пространства A.*

Доказательство. Однозначность определения изоморфным отображением σ отображения σ' почти непосредственно следует из второго равенства. Для доказательства существования отображения σ' поступим следующим образом. По теореме 2 (§ 6), изоморфное отображение σ группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$ индуцирует изоморфное отображение группы $\mathrm{T}(F, A)$ на группу $\mathrm{T}(G, B)$. Теперь проведем те же рассуждения, какими мы пользовались при доказательстве теоремы об изоморфном отображении в § 5. Если S есть отличное от 0 и A подпространство F-пространства A, то положим $S^{\nu} = J^{+}([\Delta(S)^{2}]^{\sigma}) = J^{+}([\Delta(S)^{\sigma}]^{2})$. Поскольку σ индуцирует изоморфное отображение группы $\mathrm{T}(F, A)$ на группу $\mathrm{T}(G, B)$, из теоремы 4 (§ 4) следует, что ν является взаимно однозначным отображением совокупности отличных от 0 и A подпространств F-пространства A на совокупность отличных от 0 и B подпространств G-пространства B; в силу теоремы 2 (§ 4), ν сохраняет соотношение расположения между. Следовательно, по лемме 2 (§ 5), ν индуцируется либо проективным, либо дуальным отображением, которое обозначим через σ'. Из теоремы 3 (в) (§ 4) легко вытекает, что σ' удовлетворяет и первому из наших требований,

$$\Delta(S^{\sigma'}) = \Delta(S)^{\sigma}.$$

Доказательство структурной теоремы. Если существует изоморфное отображение группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$, то, в силу предложения 3, существует либо проективное, либо дуальное отображение F-пространства A на G-пространство B. Обратно, пусть существует проективное или дуальное отображение F-пространства A на G-пространство B. Если существует проективное отображение, то, по первой основной теореме проективной геометрии (гл. III, § 1), существует полулинейное проективное преобразование F-пространства A на G-пространство B, и, следовательно, существует индуцированное изоморфное отображение первого рода группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$. Если же существует дуальное отображение F-пространства A на G-пространство B, то из леммы 2 (гл. IV, § 1) следует существование инверсно полулинейного преобразования сопряженного пространства (A^{*}, F) на линейное многообразие (G, B), а из теоремы существования (гл. IV, § 1) вытекает конечность ранга $r(A)$. Поэтому, в силу следствия 1, существует индуцированное изоморфное отображение второго рода группы $\Lambda(F, A)$

на группу $\Lambda(G, B)$. Таким образом, в обоих случаях группы $\Lambda(F, A)$ и $\Lambda(G, B)$ изоморфны.

Лемма 2. *Если ранг $r(A)$ конечен и ν — естественное изоморфное отображение группы $\Lambda(F, A)$ на группу $\Lambda(A^*, F)$, то $\Delta(S)^\nu = \Delta[E(S)]$ для каждого подпространства S F-пространства A.*

Доказательство. Прежде всего напомним, что $E(S)$ есть совокупность всех таких линейных форм f из A^*, что $Sf = 0$. Заметим, кроме того, что ν отображает всякое полулинейное преобразование F-пространства A на полулинейное преобразование сопряженного пространства A^*, имеющее ту же самую F-компоненту. Отсюда, в частности, следует, что ν отображает линейные преобразования на линейные преобразования; очевидно также, что при изоморфном отображении образом инволюции будет инволюция. Поэтому, если σ — инволюция из $\mathrm{T}(F, A)$, то $\sigma^\nu = \sigma^*$, где через * обозначено естественное инверсно изоморфное отображение группы $\Lambda(F, A)$ на группу $\Lambda(A^*, F)$, определенное нами равенством (3).

Инволюция σ тогда и только тогда принадлежит $\Delta(S)^+$, когда $S = J^+(\sigma)$; это эквивалентно следующим двум условиям: $s^\sigma = s$ для каждого s из S и $x^\sigma \equiv -x \pmod S$ для каждого x из A.

Отсюда следует, что если линейная форма f принадлежит $E(S)$, то

$$0 = (x + x^\sigma) f = xf + x^\sigma f = xf + xf^{\sigma^*} = x(f + f^{\sigma^*}) \text{ для каждого } x \text{ из } A;$$

таким образом, $f^{\sigma^*} = -f$ для каждого f из $E(S)$. Если теперь f — произвольная линейная форма из A^* и s — элемент подпространства S, то

$$s(f - f^{\sigma^*}) = sf - sf^{\sigma^*} = sf - s^\sigma f = sf - sf = 0,$$

ибо $S = J^+(\sigma)$; следовательно, линейная форма $f - f^{\sigma^*}$ принадлежит $E(S)$. Тем самым показано, что если $S = J^+(\sigma)$, то $E(S) = J^-(\sigma^*)$.

Обратно, пусть $E(S) = J^-(\sigma^*)$. Это эквивалентно следующим свойствам:

$$f^{\sigma^*} = -f \text{ для каждого } f \text{ из } E(S) \text{ и } g^{\sigma^*} \equiv g \pmod{E(S)}$$

для каждого g из A^*.

Поэтому, если s — некоторый элемент подпространства S и g — линейная форма из A^*, то

$$0 = s(g - g^{\sigma^*}) = sg - sg^{\sigma^*} = sg - s^\sigma g = (s - s^\sigma) g.$$

Следовательно, каждая линейная форма над A отображает элемент $s - s^\sigma$ на 0. Но, в силу предложения 2 (гл. II, § 3), это означает, что $s - s^\sigma = 0$; таким образом, $s^\sigma = s$ для каждого s из S. Далее, если a — произвольный элемент F-пространства A и

f — линейная форма из $E(S)$, то

$$(a+a^{\sigma})f = af + a^{\sigma}f = af + af^{\sigma^*} = a(f+f^{\sigma^*}) = a0 = 0,$$

так что $a+a^{\sigma}$ принадлежит подпространству $S[E(S)]$, которое равно S в силу предложения 2 (гл. II, § 3). Отсюда следует, что $J^{+}(\sigma) = S$.

Таким образом, мы показали, что σ тогда и только тогда будет такой инволюцией, что $S = J^{+}(\sigma)$, когда σ^* будет инволюцией и $E(S) = J^{-}(\sigma^*)$. Но это эквивалентно тому, что

$$[\Delta(S)^{+}]^* = \Delta[E(S)]^{-};$$

из полученного равенства легко вывести утверждение леммы, принимая во внимание, что на инволюциях естественное изоморфное и естественное инверсно изоморфное отображения совпадают.

Доказательство теоремы об изоморфном отображении. Начнем с доказательства единственности (в указанном выше смысле). Пусть α, β — сингулярные автоморфизмы группы $\Lambda(F, A)$, а γ, δ — индуцированные изоморфные отображения группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$, и пусть $\alpha\gamma = \beta\delta = \sigma$. Тогда, в силу предложений 1 и 3, существует такое проективное или дуальное отображение σ', что

$$\Delta(S^{\sigma'}) = \Delta(S)^{\sigma} = \Delta(S)^{\gamma} = \Delta(S)^{\delta}$$

для каждого подпространства S F-пространства A. Если γ — индуцированное изоморфное отображение первого рода, то γ индуцируется некоторым полулинейным преобразованием τ линейного многообразия (F, A) на линейное многообразие (G, B), так что

$$\Delta(S^{\sigma'}) = \Delta(S)^{\gamma} = \tau^{-1}\Delta(S)\tau = \Delta(S^{\tau})$$

и, следовательно, σ' является проективным отображением, индуцированным полулинейным преобразованием τ. Если же γ — индуцированное изоморфное отображение второго рода, то ранг $r(A)$ конечен и существует такое инверсно полулинейное преобразование ω сопряженного пространства (A^*, F) на линейное многообразие (G, B), что γ отображает элемент η группы $\Lambda(F, A)$ на $\eta^{\nu\omega} = \omega^{-1}\eta\,\omega$, где ν — естественное изоморфное отображение группы $\Lambda(F, A)$ на группу $\Lambda(A^*, F)$. Отсюда и из леммы 2 вытекает, что

$$\Delta(S^{\sigma'}) = \Delta(S)^{\gamma} = \omega^{-1}\Delta(S)^{\nu}\omega = \omega^{-1}\Delta[E(S)]\,\omega = \Delta[E(S)^{\omega}]$$

и, следовательно, по теореме 3 (гл. II, § 3), σ' является дуальным отображением, при котором образом подпространства S будет подпространство $E(S)^{\omega}$. Полученные результаты, которыми мы

в дальнейшем будем пользоваться, можно сформулировать следующим образом:

(I) *Если* α *— сингулярный автоморфизм группы* $\Lambda(F, A)$ *и* γ *— изоморфное отображение группы* $\Lambda(F, A)$ *на группу* $\Lambda(G, B)$, *индуцированное полулинейным преобразованием* τ *F-пространства A на G-пространство B, то*

$$\Delta(S^{\tau}) = \Delta(S)^{\alpha\gamma}$$

для каждого подпространства S F-пространства A.

(II) *Если* α *— сингулярный автоморфизм группы* $\Lambda(F, A)$ *и* γ *— изоморфное отображение группы* $\Lambda(F, A)$ *на группу* $\Lambda(G, B)$, *индуцированное инверсно полулинейным преобразованием* ω *сопряженного пространства A* на G-пространство B, то*

$$\Delta[E(S)^{\omega}] = \Delta(S)^{\alpha\gamma}$$

для каждого подпространства S F-пространства A.

Применим эти утверждения к нашему изоморфному отображению $\sigma = \alpha\gamma = \beta\delta$ и к соответствующему ему отображению σ', которое является либо проективным, либо дуальным. Мы получаем, что σ' тогда и только тогда будет проективным отображением, когда γ и δ являются индуцированными изоморфными отображениями первого рода, причем γ и δ порождаются полулинейными преобразованиями, индуцирующими проективное отображение σ'; аналогично, σ' тогда и только тогда будет дуальным отображением, когда γ и δ являются индуцированными изоморфными отображениями второго рода, причем γ и δ порождаются инверсно полулинейными преобразованиями, индуцирующими дуальное отображение σ'.

Если γ и δ индуцируются соответственно полулинейными преобразованиями γ' и δ', то

$$\Delta(S^{\gamma'}) = \Delta(S)^{\alpha\gamma} = \Delta(S)^{\beta\delta} = \Delta(S^{\delta'})$$

для каждого подпространства S F-пространства A. Полулинейные преобразования γ' и δ' индуцируют одно и то же проективное отображение F-пространства A на G-пространство B, и, следовательно, они отличаются друг от друга лишь на тривиальное полулинейное преобразование F-пространства A (см. предложение 3, гл. III, § 1). Отсюда вытекает, что $\beta^{-1}\alpha = \delta\gamma^{-1}$ будет внутренним автоморфизмом группы $\Lambda(F, A)$, индуцированным элементом из N; этим показано, что изоморфное отображение σ по существу однозначно представимо в виде произведения сингулярного автоморфизма и индуцированного изоморфного отображения первого рода. Если же γ и δ являются индуцированными изоморфными отображениями второго рода, то подобным же образом, только опираясь на утверждение (II), можно показать, что и в этом случае

представление изоморфного отображения σ в виде произведения сингулярного автоморфизма и индуцированного изоморфного отображения будет по существу однозначным; детали доказательства мы оставляем читателю.

Пусть, наконец, нам дано некоторое изоморфное отображение σ группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$. Тогда, в силу предложения 3, существует такое проективное или дуальное отображение σ' F-пространства A на G-пространство B, что

$$\Delta(S^{\sigma'}) = \Delta(S)^{\sigma}$$

для каждого подпространства S F-пространства A.

Если σ' – проективное отображение, то, по первой основной теореме проективной геометрии (гл. III, § 1), существует такое полулинейное преобразование τ F-пространства A на G-пространство B, что $S^{\tau} = S^{\sigma'}$ для каждого подпространства S. Полулинейное преобразование τ индуцирует изоморфное отображение γ группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$; из утверждения (I) вытекает, что

$$\Delta(S)^{\sigma} = \Delta(S^{\sigma'}) = \Delta(S^{\tau}) = \Delta(S)^{\gamma}$$

для каждого подпространства S F-пространства A. Отсюда и из предложения 1 следует, что $\sigma\gamma^{-1}$ является сингулярным автоморфизмом группы $\Lambda(F, A)$.

Если же σ' – дуальное отображение, то, по теореме существования (гл. IV, § 1), ранг $r(A)$ конечен, а из леммы 2 (гл. IV, § 1) следует существование такого инверсно полулинейного преобразования ω сопряженного пространства A^* на G-пространство B, что $E(S)^{\omega} = S^{\sigma'}$ для каждого подпространства S F-пространства A. Изоморфное отображение δ группы $\Lambda(F, A)$ на группу $\Lambda(G, B)$, индуцированное инверсно полулинейным преобразованием ω, удовлетворяет, в силу утверждения (II), условию

$$\Delta(S)^{\sigma} = \Delta(S^{\sigma'}) = \Delta[E(S)^{\omega}] = \Delta(S)^{\delta}$$

для каждого подпространства S F-пространства A. Но в таком случае, в силу предложения 1, $\sigma\delta^{-1}$ является сингулярным автоморфизмом группы $\Lambda(F, A)$, и этим наша теорема полностью доказана.

Читателю мы предлагаем исследовать возможность построения другого доказательства теоремы об изоморфном отображении, которое в большей степени использовало бы результаты § 5, чем наше доказательство; ср. доказательство структурной теоремы [1]).

[1]) Результаты § 5 были использованы лишь при доказательстве предложения 3.—*Прим. перев.*

Группа автоморфизмов группы $\Lambda(F, A)$, обозначаемая через $A(\Lambda)$. Эта группа содержит подгруппу $A_s(\Lambda)$ сингулярных автоморфизмов, которая является нормальным делителем в $A(\Lambda)$, поскольку она состоит как раз из тех автоморфизмов группы Λ, которые индуцируют тождественный автоморфизм фактор-группы Λ/N [заметим, что N, в силу теоремы 2 (§ 6), является характеристической подгруппой группы Λ]. Кроме того, $A(\Lambda)$ содержит подгруппу $A_i(\Lambda)$ всех индуцированных автоморфизмов группы Λ и нормальный делитель $A_0(\Lambda)$, состоящий из всех внутренних автоморфизмов группы Λ [$A_0(\Lambda)$ совпадает с группой индуцированных автоморфизмов первого рода]. Очевидно, что $A_s(\Lambda) \cap A_0(\Lambda)$ также является нормальным делителем; он состоит из всех внутренних автоморфизмов, индуцированных элементами из N (см. ту часть теоремы об изоморфном отображении, в которой говорится об однозначности представления).

По теореме 2 (§ 6), каждый автоморфизм α группы Λ индуцирует автоморфизм α^τ группы T. Очевидно, что τ является (естественным) гомоморфным отображением группы $A(\Lambda)$ в группу автоморфизмов $A(T)$ группы T. В силу предложения 1, ядро гомоморфизма τ состоит только из сингулярных отображений; оно содержит нормальный делитель $A_s(\Lambda) \cap A_0(\Lambda)$, ибо каждое полулинейное преобразование из N перестановочно с линейными преобразованиями. Легко проверить, что τ отображает сингулярные автоморфизмы на сингулярные автоморфизмы, индуцированные автоморфизмы первого и второго рода на индуцированные автоморфизмы того же рода и что каждый индуцированный автоморфизм группы T является образом, при гомоморфизме τ, некоторого индуцированного автоморфизма группы Λ.

Рассмотрим теперь сингулярный автоморфизм α и внутренний автоморфизм β группы Λ. Их коммутатор содержится, очевидно, в $A_s(\Lambda) \cap A_0(\Lambda)$, и, следовательно, $\alpha^\tau \beta^\tau = \beta^\tau \alpha^\tau$. Это показывает, что при гомоморфизме τ образами сингулярных автоморфизмов группы Λ являются такие сингулярные автоморфизмы группы T, которые перестановочны с каждым индуцированным автоморфизмом первого рода группы T. В то же время из примера, приведенного в § 5, видно, что не все сингулярные автоморфизмы группы T обладают этим свойством. Отсюда следует, что в общем случае при гомоморфизме τ группа $A(\Lambda)$ отображается на собственную часть группы $A(T)$ и, в частности, подгруппа $A_s(\Lambda)$ отображается на собственную часть подгруппы $A_s(T)$.

ГЛАВА VII

ВНУТРЕННЯЯ ХАРАКТЕРИСТИКА СИСТЕМЫ ПОДПРОСТРАНСТВ ЛИНЕЙНОГО МНОГООБРАЗИЯ

Совокупность $S = S(A) = S(F, A)$ подпространств линейного многообразия (F, A) представляет собой проективную геометрию, определяемую этим линейным многообразием; основными соотношениями между элементами этой проективной геометрии являются такие соотношения и операции, связывающие подпространства, как $U < V$, $U \cap V$, $U + V$. В настоящей главе будут перечислены те свойства указанных соотношений, которые полностью характеризуют систему S как совокупность подпространств линейного многообразия.

Задача, решению которой посвящена эта глава, известна под различными названиями, например «аксиоматизация геометрии», «введение координат в проективное пространство» и т. д. Это единственная глава проективной геометрии, в которой можно пользоваться лишь синтетическими методами, ибо основной целью является здесь построение алгебраического объекта (т. е. исходного линейного многообразия). После того, как это построение будет осуществлено, мы сможем пользоваться алгебраическим аппаратом всякий раз, когда нам это будет удобно.

В предыдущих главах мы довольно часто предполагали, что ранг рассматриваемого линейного многообразия больше 2. В настоящей главе мы будем рассматривать линейные многообразия, ранги которых не меньше 4 (размерности не меньше 3). Мы рассмотрим также и один специальный класс плоскостей (так называемых дезарговых плоскостей), однако очень интересного и несколько искусственного вопроса о произвольных проективных плоскостях мы касаться не будем. Связанный с этой темой материал читатель может найти в указанной ниже литературе.

ЛИТЕРАТУРА ПО АКСИОМАТИЗАЦИИ ГЕОМЕТРИИ

Артин (Artin E.), Coordinates in Affine Geometry, Reports of a Math. Coll., University of Notre Dame (2), v. 2 (1940), 15—20.

Бэр (Baer R.), Homogeneity of Projective Planes, Amer. Journal of Math., 64 (1942), 137—152.

A Unified Theory of Projective Spaces and Finite Abelian Groups, Trans. Amer. Math. Soc., 52 (1942), 283—343.

Биркгоф (Birkhoff G.), Combinatorial Relations in Projective Geometry, Ann. of Math., 36 (1935), 743—748.
Теория структур, М., 1952.
Боттема (Bottema O.), De elementaire meetkunde van het platte vlak, Groningen—Batavia, 1938.
Веблен и Янг (Veblen O., Young J. W.), Projective Geometry, v. 1, 2, Boston, 1918—1938.
Гессенберг (Hessenberg G. W.), Grundlagen der Geometrie, Leipzig, 1930.
Гильберт Д. (Hilbert D.), Основания геометрии, М.—Л., 1948.
Глаголев Н. А.*, Проективная геометрия, М.—Л., 1936.
Ефимов Н. В.*, Высшая геометрия, М.—Л., 1945.
Йольмслев (Hjelmslev J.), Grundlag for den projektive Geometrie, Kjobenhavn, 1933.
Коксетер (Coxeter H. S. M.), The Real Projective Plane, New York, 1949.
Копейкина Л. И.*, Свободные разложения проективных плоскостей, Изв. АН СССР, сер. матем., 9 (1945), 495—526.
Кёте (Köthe G.), Die Theorie der Verbände, ein neuer Versuch zur Grundlegung der Algebra und der projectiven Geometrie, Jahresberichte der Deutschen Math. Ver., 47 (1937), 125—144.
Леви (Levi F.), Geometrische Konfigurationen, Leipzig, 1929.
Либман (Liebmann H.), Synthetische Geometrie, Leipzig und Berlin, 1934.
Менгер (Menger K.), New Foundations of Projective and Affine Geometry, Ann. of Math., 37 (1936), 456—482.
Моуфанг (Moufang R.), Alternativkörper und der Satz vom vollständigen Vierseit (D_9), Abhandlungen aus dem math. Seminar der Hamburgischen Universität, 9 (1933), 207—222.
Нейман (von Neumann J.), Continuous Geometry, Princeton, 1936—1937.
Паш (Pasch M.), Vorlesungen über neuere Geometrie, mit einem Anhang: die Grundlegung der Geometrie in historischer Entwicklung von Max Dehn, Berlin, 1926.
Рейдемейстер (Reidemeister K.), Vorlesungen über Grundlagen der Geometrie, Berlin, 1930.
Робинсон (G. de B. Robinson), The Foundations of Geometry, Toronto, 1940.
Скорняков Л. А.*, Натуральные тела веблен-веддербарновой проективной плоскости, Изв. АН СССР, сер. матем., 13 (1949), 447—472; Проективные плоскости, Успехи матем. наук, VI, вып. 6 (1951), 112—154.
Томсен (Thomsen G.), Grundlagen der Elementargeometrie in gruppentheoretischer Behandlung, Berlin und Leipzig, 1933.
Хейтинг (Heyting A.), Intuitionistische axiomatiek der projektieve meetkunde, Groningen, 1925.

Хермеш, Кёте (Hermes H., Köthe G.), Die Theorie der Verbände, Enzyklopädie der math. Wiss., I, 1, 13.

Хефтер (Hefftter L.), Grundlagen und analytischer Aufbau der Geometrie, 2 Aufl., Leipzig, 1950.

Холл (Hall M.), Projective Planes, Trans. Amer. Math. Soc., 54 (1943), 229—277.

Шур (Schur F.), Grundlagen der Geometrie, Leipzig und Berlin, 1909.

§ 1. Основные понятия, аксиомы и простейшие свойства

Отправной точкой наших рассмотрений является понятие *частично упорядоченного множества*. Это есть множество S элементов, в котором определено соотношение «$\leqslant$». Из очевидных соображений мы будем обозначать элементы множества S большими буквами, а вместо выражения «$U \leqslant V$» использовать такие выражения, как «U является частью V», «U содержится в V», «U лежит на V», «V содержит U», «V проходит через U». Если $U \leqslant V$ и в то же время $U \neq V$, то мы будем иногда писать $U < V$.

Соотношение «$\leqslant$» (включения или упорядочения) удовлетворяет следующим естественным аксиомам:

I. *$U \leqslant V$ и $V \leqslant U$ тогда и только тогда, когда $U = V$.*

II. *Из $U \leqslant V$ и $V \leqslant W$ следует $U \leqslant W$.*

Это аксиомы частично упорядоченного множества. Заметим, что в частично упорядоченном множестве S могут существовать такие пары элементов U и V, между которыми не имеют места ни соотношение $U \leqslant V$, ни соотношение $V \leqslant U$, и что поэтому из условия «U не содержится в V» может не следовать соотношение $V < U$.

Определение 1. *Пусть Θ есть некоторое множество элементов из S, и пусть элемент*

U из S обладает следующими свойствами:

(а′) *$U \leqslant X$ для каждого X из Θ;*

(б′) *если M — такой элемент из S, что $M \leqslant X$ для каждого X из Θ, то $M \leqslant U$.*

Тогда положим

$$U = \prod_{X \in \Theta} X.$$

V из S обладает следующими свойствами:

(а″) *$X \leqslant V$ для каждого X из Θ;*

(б″) *если N — такой элемент из S, что $X \leqslant N$ для каждого X из Θ, то $V \leqslant N$.*

Тогда положим

$$V = \sum_{X \in \Theta} X.$$

V часто называют наименьшей верхней гранью множества Θ, а U — наибольшей нижней гранью этого множества. Однако нам удобнее называть U пересечением, а V суммой элементов множества Θ. В случае, когда Θ состоит из небольшого числа элементов,

мы будем пользоваться такими обозначениями, как

$H \cap K$, $H \cap K \cap L$ и т. д. для U; $H + K$, $H + K + L$ и т. д. для V.

Легко видеть, что существуют самое большее одно пересечение и самое большее одна сумма элементов множества Θ. Однако доказать существование по крайней мере одного элемента, являющегося пересечением (или суммой) элементов данного множества Θ, нельзя, и поэтому мы вводим следующую дополнительную аксиому.

III. *Если Θ есть непустое подмножество множества S, то существуют пересечение $\prod_{X \in \Theta} X$ и сумма $\sum_{X \in \Theta} X$ элементов из Θ.*

Из этой аксиомы, в частности, следует существование пересечения 0 и суммы A всех элементов множества S. (Заметим, что обычно в теории частично упорядоченных множеств сумма всех элементов обозначается символом 1; однако ясно, почему нам, в соответствии с принятым в предыдущих главах обозначением, удобнее использовать символ A.)

Легко проверить, что сумма элементов множества Θ совпадает с пересечением совокупности всех элементов, каждый из которых содержит все элементы из Θ, и что пересечение элементов множества Θ совпадает с суммой всех элементов, содержащихся в каждом элементе из Θ. Используя это замечание, можно показать, что вместо аксиомы III достаточно было бы потребовать либо существования элемента A и всех пересечений, либо существования элемента 0 и всех сумм.

Очевидно, что множество всех подпространств данного линейного многообразия с существующим в этом множестве соотношением включения удовлетворяет аксиомам I—III и что наши определения суммы и пересечения согласуются с аналогичными определениями, введенными в теории линейных многообразий.

IV. *Если U, V, W — элементы множества S и если $U \leqslant V$, то*

$$V \cap (U + W) = U + (V \cap W).$$

Эта аксиома в точности совпадает с законом Дедекинда (см. гл. II, § 1). Этот закон часто называют модулярным законом. Мы, как правило, будем называть аксиому IV законом Дедекинда. Теперь легко убедиться в эквивалентности следующих соотношений:

$$X \cap Y = X, \quad X \leqslant Y, \quad X + Y = Y\ ^{1}).$$

V. *Если U — произвольный элемент из S, то в множестве S существует такой элемент V, что $0 = U \cap V$ и $A = U + V$.*

---

[1]) Это утверждение непосредственно следует из определений. — *Прим. перев.*

Этой аксиоме соответствует в теории линейных многообразий теорема о дополнении (см. гл. II, § 1); мы будем аксиому V часто называть принципом дополнения. Систему, в которой выполняются аксиомы I—V, обычно называют «полной модулярной (или дедекиндовой) структурой с дополнениями».

В системе, удовлетворяющей аксиомам I—V, имеет место следующий *обобщенный принцип дополнения*:

Если $U \leqslant V \leqslant W$, то в S существует такой элемент T, что $U = V \cap T$ и $W = V + T$.

Доказательство. По аксиоме V, в S существует такой элемент H, что $0 = V \cap H$ и $A = V + H$. Пусть $T = U + (H \cap W)$. Тогда, используя закон Дедекинда, мы из соотношения $U \leqslant V$ выведем, что

$$V \cap T = V \cap [U + (H \cap W)] = U + (V \cap H \cap W) = U + 0 = U,$$

а из соотношения $U \leqslant V \leqslant W$, вновь используя закон Дедекинда, получаем, что

$$V + T = V + U + (H \cap W) = V + (H \cap W) = W \cap (V + H) = W \cap A = W.$$

Определение 2. *Если $U < V$ и если из $U \leqslant X < V$ следует равенство $X = U$, то будем говорить, что V является точкой по модулю U.*

Вместо выражения «V является точкой по модулю U» мы обычно будем употреблять выражение «V/U является точкой», а в случае, когда V является точкой по модулю 0, будем кратко называть V точкой. Наши определение и название полностью согласуются с терминами, которыми мы пользовались раньше (см., в частности, гл. II, §§ 1 и 2).

VI. *Если U — отличный от 0 элемент множества S, то U содержит хотя бы одну точку.*

Совершенно очевидно, что аксиома VI выполняется в множестве $S(A)$ всех подпространств линейного многообразия (F, A).

Лемма 1. *Если $U < V$, то существует такая точка P, что $P \leqslant V$, P не содержится в U и, следовательно, $U + P$ содержится в V, а также является точкой по модулю U.*

Доказательство. Так как $0 \leqslant U < V$, то, в силу обобщенного принципа дополнения, существует такой элемент W, что $0 = U \cap W$ и $V = U + W$. Поскольку $U < V$, мы имеем $W \neq 0$. Следовательно, согласно аксиоме VI, в W содержится некоторая точка P. Если P содержится и в U, то $P \leqslant U \cap W = 0$, что невозможно. Таким образом, мы показали, что $P \leqslant V$ и P не содержится в U; отсюда следует, очевидно, что $U < U + P \leqslant V$. Пусть, наконец, X — произвольный элемент множества S, удовлетворяющий условию $U \leqslant X < U + P$. Тогда P не содержится в X и, следовательно, $P \cap X < P$. Но P является точкой; поэтому $P \cap X = 0$. Отсюда,

используя закон Дедекинда, мы получаем, что

$$X = X \cap (U + P) = U + (X \cap P) = U + 0 = U;$$

этим доказано, что $(U+P)/U$ будет точкой.

VII. *Если Θ — произвольное множество элементов из S, P — точка из S и если $P \leqslant \sum_{X \in \Theta} X$, то в Θ существует конечное число таких элементов $X_1, \ldots, X_k$, что $P \leqslant \sum_{i=1}^{k} X_i$.*

Проверка аксиомы VII в системе $S(F, A)$. Каждая точка P из $S(F, A)$ имеет вид Fp; поэтому точка P тогда и только тогда является частью суммы подпространств X, принадлежащих Θ, когда в этой сумме содержится элемент p. Но сумма подпространств X из Θ состоит из всех конечных сумм вида $x_1 + \ldots + x_k$, где x_i принадлежит X_i, а X_i — подпространства, принадлежащие Θ. Теперь уже видно, как завершается проверка справедливости в системе $S(F, A)$ аксиомы VII.

Лемма 2. *Если Θ — некоторое множество элементов из S и если $U < V \leqslant \sum_{X \in \Theta} X$, то в Θ существует конечное число таких элементов $X_1, \ldots, X_k$, что*

$$U \cap \sum_{i=1}^{k} X_i < V \cap \sum_{i=1}^{k} X_i.$$

Доказательство. Из леммы 1 следует существование точки P, содержащейся в V и не содержащейся в U. В силу аксиомы VII, существует конечное число таких элементов $X_1, \ldots, X_k$ из Θ, что $P \leqslant \sum_{i=1}^{k} X_i$. В таком случае

$$U \cap \sum_{i=1}^{k} X_i < V \cap \sum_{i=1}^{k} X_i,$$

ибо точка P содержится в правой части включения и не содержится в левой.

Следствие 1. *Если Θ — подмножество множества S, $U \leqslant X$ для каждого X из Θ, $V \leqslant \sum_{X \in \Theta} X$ и V/U — точка, то в Θ существует конечное число таких элементов $X_1, \ldots, X_k$, что $V \leqslant \sum_{i=1}^{k} X_i$.*

Доказательство. Из леммы 2 следует существование в множестве Θ конечного числа таких элементов $X_1, \ldots, X_k$, что

$$U = U \cap \sum_{i=1}^{k} X_i < V \cap \sum_{i=1}^{k} X_i \leqslant V.$$

Но V/U — точка; поэтому $V = V \cap \sum_{i=1}^{k} X_i$, т. е. $V \leqslant \sum_{i=1}^{k} X_i$.

VIII. *Если P и Q — различные точки множества S, то существует такая отличная от P и Q точка R, что $R \leqslant P+Q$.*

Легко видеть, что требования, налагаемые в аксиоме VIII на «третью» точку R прямой $P+Q$, эквивалентны следующему соотношению:

$$P+Q=Q+R=R+P.$$

Проверка аксиомы VIII в системе $S(A)$. Если P и Q — различные точки F-пространства A, то существуют такие отличные от 0 элементы p и q, что $P=Fp$, $Q=Fq$; точка $R=F(p+q)$ является требуемой третьей точкой прямой $P+Q$.

Ограничение, налагаемое аксиомой VIII, не является сколько-нибудь существенным, поскольку каждую систему, удовлетворяющую аксиомам I — VII, можно единственным (и естественным) образом «разложить» на компоненты, обладающие свойствами I — VIII; строение этих компонент определяет строение исходной системы. Детали такого разложения изложены в работе Фринка [1], в которой можно также найти дополнительные ссылки.

Лемма 3. *Если $U < V < W$, то в S существуют такие два различных элемента T' и T'', что $U=V\cap T'=V\cap T''$, $W=V+T'=V+T''$.*

Доказательство. В силу обобщенного принципа дополнения, в S существует такой элемент T, что $U=V\cap T$ и $W=V+T$; поскольку $U<V<W$, мы имеем $U<T<W$. Воспользуемся теперь леммой 1, в силу которой существуют такие точки P, Q, что $P\leqslant T$, P не содержится в U, $Q\leqslant V$ и Q не содержится в U. Так как $U<U+P\leqslant T$, то, вновь используя обобщенный принцип дополнения, мы найдем в S элемент H, удовлетворяющий условиям $U=H\cap(U+P)$, $T=H+U+P=H+P$.

Точки P и Q, очевидно, различны; поэтому, согласно аксиоме VIII, существует такая третья точка R, что $P+Q=Q+R=R+P$. Положим $T^*=H+R$.

Прежде всего заметим, что точка Q не содержится в T, ибо в противном случае Q содержалась бы в $T\cap V=U$. Если хотя бы одна из точек P и Q лежит на T^*, то, поскольку $P+R=R+Q$, они обе должны лежать на T^*. Но тогда $T=H+P\leqslant H+R=T^*$, и так как элемент T во всяком случае не содержит точку Q, то $H\leqslant T=H+P<H+R$. Отсюда, в частности, вытекает, что $H+R$ является точкой по модулю H (см. лемму 1 и ее доказательство). Поэтому $H=H+P$, т. е. $P\leqslant H$. Но отсюда следует, что

$$P\leqslant H\cap(U+P)=U,$$

а это противоречит выбору точки P. Таким образом, ни одна из точек P, Q не лежит на T^*.

Отсюда, в частности, вытекает, что $T\neq T^*$. В то же время

$$V+T^*=V+H+R=V+Q+R+H=V+Q+P+H=V+T=W;$$

кроме того, используя закон Дедекинда, мы получаем, что

$$V \cap T^* = V \cap (H + R) = V \cap (H + R) \cap (T + R) =$$
$$= V \cap (H + P + R) \cap (H + R) = V \cap (H + Q + P) \cap (H + R) =$$
$$= [Q + (V \cap T)] \cap (H + R) = (Q + U) \cap (H + R) =$$
$$= U + [Q \cap (H + R)] = U,$$

поскольку точка Q не лежит на $T^* = H + R$. Этим лемма 3 полностью доказана.

Определение 3. *Если U, V — элементы множества S и если $U \leqslant V$; то V/U есть совокупность всех таких элементов X из S, что $U \leqslant X \leqslant V$.*

Очевидно, что V/U является частично упорядоченным множеством относительно того же соотношения «$\leqslant$», какое определено во всем S. Нулевым элементом множества V/U будет U, а «A»-элементом множества V/U будет V. Используя леммы 1—3 и следствие 1, легко доказать

Предложение 1. *V/U удовлетворяет всем аксиомам* I—VIII.

Замечание о принципе двойственности. В гл. IV было показано, что каждое линейное многообразие конечного ранга двойственно некоторому, вообще говоря отличному от него, линейному многообразию и что линейные многообразия бесконечного ранга этим свойством не обладают. Следовательно, теория линейных многообразий лишена двойственности; для восстановления этой двойственности мы должны были бы исключить из рассмотрения линейные многообразия бесконечного ранга. Поэтому невозможно дать двойственную себе систему аксиом проективной геометрии, которая охватывала бы проективные геометрии, определяемые линейными многообразиями бесконечного ранга. Двойственную себе систему аксиом проективной геометрии конечной размерности можно найти в работах Менгера [1] и Эссэра [1].

§ 2. Зависимые и независимые точки

В дальнейшем мы будем всюду предполагать, что рассматриваемое множество S удовлетворяет всем аксиомам I—VIII; при ссылке на эти аксиомы мы будем указывать лишь их номер. Конечно, не всегда нам будет необходимо выполнение всех указанных аксиом, и читателю полезно проверять, какими из них мы действительно пользуемся при рассмотрении каждого отдельного вопроса.

Предложение 1. *Каждый элемент X множества S является суммой точек, содержащихся в X.*

Здесь мы, как это обычно делается, полагаем, что 0 является суммой пустого множества точек.

Доказательство. Обозначим через Y сумму всех точек, содержащихся в X. В силу обобщенного принципа дополнения, в S существует такой элемент Z, что $X = Y + Z$ и $0 = Y \cap Z$. Если бы элемент Z был отличен от 0, то, по аксиоме VI, существовала бы точка $P \leqslant Z$. Очевидно, что P содержится также и в X. Отсюда и из определения элемента Y вытекает, что $P \leqslant Y$. Таким образом, $P \leqslant Y \cap Z = 0$, и мы пришли к противоречию. Следовательно, $Z = 0$, и $X = Y$ является суммой точек, содержащихся в X.

Определение 1. *Точка P называется зависимой от множества точек Φ, если* $P \leqslant \sum_{X \in \Phi} X$.

Предложение 2. *Соотношение зависимости точек обладает следующими свойствами:*

(а) *Нет точек, зависящих от пустого множества.*

(б) *Если точка P зависит от множества точек Φ и если Φ является подмножеством множества точек Θ, то P зависит от Θ.*

(в) *Если точка P зависит от множества точек Φ, то P зависит от конечного подмножества множества Φ.*

(г) *Если точка P зависит от множества точек Φ и если каждая точка из Φ зависит от множества точек Θ, то P зависит от Θ.*

(д) *Если точка P зависит от конечного множества точек $P_1, \ldots, P_k$, но не зависит ни от одного собственного подмножества этого множества, то точка P_1 зависит от $P, P_2, \ldots, P_k$.*

(е) *Каждая точка зависит от самой себя.*

Доказательство. Если точка P зависит от множества точек Φ и если каждая точка из Φ зависит от множества точек Θ, то

$$P \leqslant \sum_{X \in \Phi} X \leqslant \sum_{Y \in \Theta} Y,$$

ибо для каждой точки X из Φ имеет место соотношение $X \leqslant \sum_{Y \in \Theta} Y$; этим доказано, что точка P зависит от Θ. Тем самым мы убедились в справедливости утверждения (г). Утверждение (в) непосредственно следует из аксиомы VII. Утверждения (а), (б) и (е) очевидны.

Предположим, наконец, что точка P зависит от конечного множества точек $P_1, \ldots, P_k$, но не зависит ни от одного его собственного подмножества. Тогда

$$P \leqslant \sum_{i=1}^{k} P_i \text{ и } P \text{ не содержится в } \sum_{i=2}^{k} P_i.$$

Используя закон Дедекинда, мы выводим, что

$$P + \sum_{i=2}^{k} P_i = \left[P + \sum_{i=2}^{k} P_i\right] \cap \sum_{i=1}^{k} P_i = \sum_{i=2}^{k} P_i + \left[P_1 \cap \left(P + \sum_{i=2}^{k} P_i\right)\right].$$

Так как точка P не содержится в $\sum_{i=2}^{k} P_i$, то

$$\sum_{i=2}^{k} P_i < P + \sum_{i=2}^{k} P_i;$$

отсюда и из предыдущего равенства вытекает, что

$$P_1 \cap [P + \sum_{i=2}^{k} P_i] \neq 0.$$

Но P_1 — точка; следовательно, последнее пересечение равно P_1. Тем самым показано, что

$$P_1 \leqslant P + \sum_{i=2}^{k} P_i,$$

чем и завершается доказательство утверждения (д). Попутно показано, что $\sum_{i=1}^{k} P_i = P + \sum_{i=2}^{k} P_i$.

Замечание 1. Утверждения (а) — (е) представляют собой так называемые аксиомы алгебраической зависимости, которыми мы неявно пользовались в § 2 гл. II. Подробную теорию алгебраической зависимости читатель может найти в работе Мак-Лейна [1].

Определение 2. *Множество точек Φ называется независимым, если в Φ не существует ни одной точки, зависящей от остальных точек этого множества.*

Определение 3. *Множество точек Φ называется базисом элемента E из S, если оно независимо и если E является суммой всех точек, принадлежащих Φ.*

Теорема 1. *Каждый элемент множества S обладает базисом.*

Теорема 2. *Любые два базиса элемента E из S состоят из одного и того же числа точек; это (конечное или бесконечное) число называется рангом $r(E)$ элемента E.*

Доказательства этих двух теорем очень похожи на доказательства соответствующих теорем из § 2 гл. II; поэтому мы предоставляем читателю самому убедиться в справедливости теорем 1 и 2.

Заметим, что элемент L множества S, ранг которого равен 2, называется прямой. Прямая L является суммой двух произвольных различных точек, содержащихся в L. Элементы, имеющие ранг 3, называются плоскостями; плоскость можно представить в виде суммы трех независимых точек.

Теорема 3. *Если ранг элемента E конечен, то конечен также ранг любого элемента, содержащегося в E. Если E' и E'' — элементы конечного ранга, то*

$$r(E') + r(E'') = r(E' + E'') + r(E' \cap E'').$$

Доказательство теоремы 3 очень похоже на доказательства соответствующих утверждений из § 2 гл. II. Поэтому мы оставляем его читателю.

Отметим, что две различные прямые, лежащие на одной плоскости, пересекаются по точке, а две различные плоскости, содержащиеся в одном элементе ранга 4, пересекаются по прямой.

Заметим, наконец, что *гиперплоскостями* мы будем называть такие элементы H, что A/H является точкой. Если элемент A имеет конечный ранг, то $r(A)=r(H)+1$; если же ранг $r(A)$ бесконечен, то $r(A)=r(H)$. Заметим, что лишь в случае, когда ранг $r(A)$ конечен, приведенное сейчас соотношение для рангов полностью характеризует гиперплоскости.

Всякий раз, когда это возможно, мы будем пользоваться соответствующей геометрической терминологией. Так, мы будем говорить, что прямые проходят через точку, несут на себе точку, пересекаются по точке и т. д.

§ 3. Теорема Дезарга

Содержание настоящего параграфа почти полностью тождественно с рассмотрениями, проводимыми в обычной трехмерной проективной геометрии. Поэтому детали отдельных доказательств мы будем опускать.

Предложение 1. *Пусть три прямые L, L', L'' (фиг. 13) проходят через одну точку P и не лежат в одной плоскости. Пусть, кроме того, Q, R — точки прямой L; Q', R' — точки прямой L' и Q'', R'' — точки прямой L'', причем ни одна из этих точек не совпадает с точкой P. Предположим, наконец, что $Q+Q'\neq R+R'$, $Q'+Q''\neq R'+R''$ и $Q''+Q\neq R''+R$. Тогда*

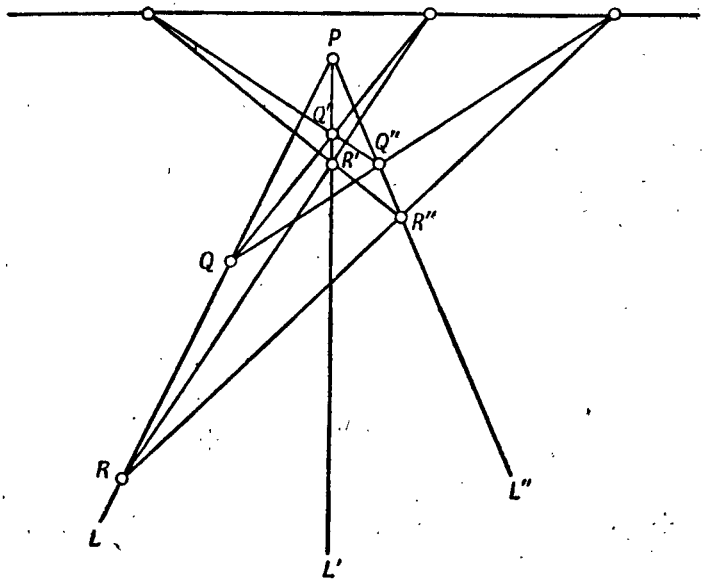
$$(Q+Q')\cap(R+R'),\ (Q'+Q'')\cap(R'+R''),\ (Q''+Q)\cap(R''+R)$$

будут коллинеарными точками.

Доказательство. Заметим прежде всего, что $L+L'$, $L'+L''$ и $L''+L$ являются тремя попарно различными плоскостями. Далее, заметим, что $Q+Q'+Q''$ и $R+R'+R''$ будут двумя различными плоскостями. Отметим, наконец, что $Q+Q'$ и $R+R'$ будут двумя различными прямыми, пересекающимися в одной точке $(Q+Q')\cap(R+R')$; из тех же соображений видно, что $(Q'+Q'')\cap(R'+R'')$ и $(Q''+Q)\cap(R''+R)$ также являются точками. Но все эти точки лежат на пересечении двух различных плоскостей $Q+Q'+Q''$ и $R+R'+R''$. Пересечением же этих плоскостей является, очевидно, прямая, поскольку они обе содержатся в элементе $L+L'+L''$, ранг которого равен 4. Тем самым предложение 1 полностью доказано.

Предложение 2. *Предположим, что $r(A)>3$. Пусть, далее, три попарно различные прямые L, L', L'' проходят через одну*

точку P, и пусть Q, R — точки прямой L, Q', R' — точки прямой L' и Q'', R'' — точки прямой L'', причем ни одна из этих точек не совпадает с точкой P. Если, наконец, $Q+Q' \neq R+R'$, $Q'+Q'' \neq R'+R''$ и $Q''+Q \neq R''+R$, то $(Q+Q') \cap (R+R')$, $(Q'+Q'') \cap (R'+R'')$ и $(Q''+Q) \cap (R''+R)$ будут коллинеарными точками.



Фиг. 13.

Предложение 2 можно обычным способом свести к предложению 1. (См., например, Веблен и Янг [1], стр. 41)[1].

Если в предложении 2 опустить условие, что $r(A) > 3$, или в предложении 1 опустить условие, что прямые L, L', L'' не компланарны, то эти предложения перестают, вообще говоря, быть верными. Именно это является отправной точкой исследований в теории проективных плоскостей (которые могут быть как дезарговыми, так и недезарговыми); упомянутая теория полностью находится вне области нашего исследования. Для наших же целей необходимо потребовать справедливости в множестве S теоремы Дезарга; поэтому мы введем следующую дополнительную аксиому.

IX. *Если три попарно различные прямые L, L', L'' проходят через одну точку P, если Q, R — точки прямой L, Q', R' — точки прямой L' и Q'', R'' — точки прямой L'', причем ни одна из этих точек не совпадает с точкой P, и если $Q+Q' \neq R+R'$,*

[1]) См. также Четверухин [1], стр. 93—94.—*Прим. перев.*

$Q'+Q''\neq R'+R''$ и $Q''+Q\neq R''+R$, то $(Q+Q')\cap(R+R')$, $(Q'+Q'')\cap(R'+R'')$ и $(Q''+Q)\cap(R''+R)$ *являются коллинеарными точками.*

Проверка аксиомы IX в системе $S(F, A)$. Если ранг F-пространства A не меньше 4, то справедливость в $S(F, A)$ аксиомы IX следует из предложения 2. Если же ранг F-пространства A меньше 4, то мы построим F-пространство $A\dotplus A$[1]), в котором содержится исходное F-пространство A и которое имеет ранг, больший 3, если только $r(A)=3$ [при $r(A)<3$ справедливость в $S(F, A)$ аксиомы IX очевидна]. Аксиома IX выполняется в $A\dotplus A$, и, следовательно, она выполняется и в подпространстве A F-пространства $A\dotplus A$. Нетрудно убедиться в справедливости аксиомы IX в системе $S(F, A)$ и прямым подсчетом; мы можем предложить читателю сделать это в качестве полезного упражнения.

Предложение 3. *Пусть множество S удовлетворяет аксиомам* I — IX. *Тогда, если P, Q, R — три попарно различные коллинеарные точки, если P', P'', Q', Q'', R', R'' — такие точки, что $P'+Q'$ и $P''+Q''$ являются различными прямыми, пересекающимися в точке R, $Q'+R'$ и $Q''+R''$ являются различными прямыми, пересекающимися в точке P, $R'+P'$ и $R''+P''$ являются различными прямыми, пересекающимися в точке Q, и если прямые $P'+P''$, $Q'+Q''$ и $R'+R''$ попарно различны, то эти три прямые $P'+P''$, $Q'+Q''$ и $R'+R''$ образуют пучок (т. е. имеют одну общую точку).*

Это предложение, двойственное теореме Дезарга, можно доказать следующим образом. Если $r(A)>3$, то нужно воспользоваться соображениями, аналогичными (с соответствующими изменениями) тем, какие используются при доказательстве предложения 2; если же $r(A)=3$, то к аксиоме IX можно применить принцип двойственности. Детали доказательства мы оставляем читателю.

§ 4. Теорема о вложении

Целью настоящего параграфа является доказательство следующего утверждения.

Теорема о вложении. *Если частично упорядоченное множество S удовлетворяет аксиомам* I — VIII *и если ранг максимального в S элемента A не меньше* 3, *то следующее условие является необходимым и достаточным для того, чтобы в S была справедлива теорема Дезарга (аксиома* IX):

[1]) F-пространство $A\dotplus A$, «прямая сумма двух экземпляров F-пространства A», состоит из всех пар (x, y), где x и y — элементы из A; сложение этих пар и умножение их на элементы тела F производятся покомпонентно. — *Прим. перев.*

IX*. *S можно вложить в строго большее частично упорядоченное множество T, удовлетворяющее аксиомам* I — VIII[1]).

Если, в частности, ранг максимального элемента A больше 3, то справедливость в S аксиомы IX вытекает из предложения 2 (§ 3); таким образом, из теоремы о вложении следует, что в указанном случае S обладает и свойством вложимости IX*. В этом состоит основная причина того, почему мы доказываем сравнительно трудную теорему о вложении, хотя можно было бы просто вместо аксиомы IX постулировать аксиому IX*.

Теоремой о вложении мы воспользуемся в ближайшем параграфе. Следующее замечание может показать, зачем нам будет нужна эта теорема. Если множество S строго содержится в множестве T, то в T существует такой элемент B, что A будет гиперплоскостью относительно B или, что то же самое, B будет точкой над A. Далее, можно построить группу элемента B над гиперплоскостью A; эта группа содержит аддитивную группу и тело[2]) линейного многообразия, система подпространств которого проективно эквивалентна исходному частично упорядоченному множеству S. (Эта группа изоморфна группе гомотетий, которую мы строили в добавлении I к гл. III.)

Из предложения 2 (§ 3) легко следует, что если справедливо свойство IX*, то справедлива и теорема Дезарга (аксиома IX), ибо максимальный элемент B объемлющей системы T удовлетворяет условию $A < B$ и, следовательно, ранг $r(B) > 3$.

Вся остальная часть настоящего параграфа (при первом чтении ее можно опустить) будет посвящена доказательству достаточности аксиомы IX. Таким образом, мы теперь будем всюду предполагать, что частично упорядоченное множество S удовлетворяет аксиомам I — IX и что ранг максимального элемента A не меньше 3. Построим сначала

Основной четырехугольник. Он состоит из четырех компланарных прямых L_o, L_r, L_s, L_t множества S, никакие три из которых не образуют пучка (фиг. 14).

Существование основного четырехугольника легко следует из существования по крайней мере трех независимых точек [ибо $r(A) \geqslant 3$] и из того, что, по аксиоме VIII, каждая прямая проходит по крайней мере через три попарно различные точки.

Любые две из четырех прямых основного четырехугольника являются различными прямыми, лежащими в одной плоскости, и, следовательно, пересекаются по точке. Для этих точек пере-

[1]) Из дальнейшего изложения видно, что здесь под строго бо́льшим частично упорядоченным множеством, удовлетворяющим аксиомам I — VIII, подразумевается такое частично упорядоченное множество, ранг максимального элемента которого строго больше ранга максимального элемента исходного частично упорядоченного множества S. — *Прим. перев.*

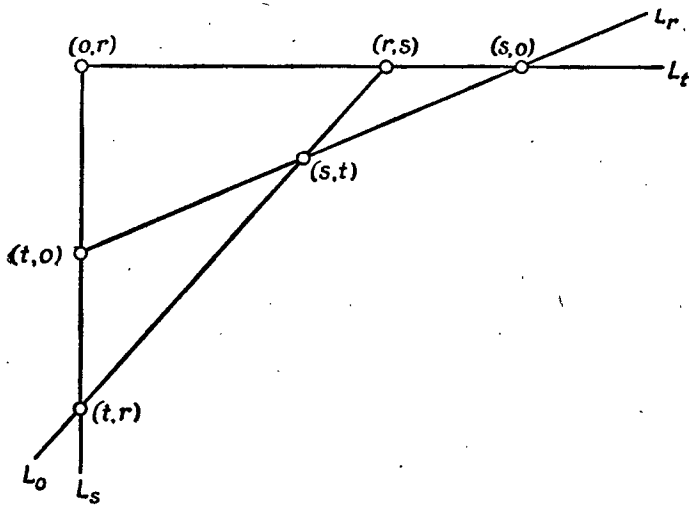
[2]) Более точно: мультипликативную группу тела. — *Прим. перев.*

сечения мы будем использовать следующее систематическое *обозначение*. Если h, k, m, n — некоторая перестановка символов o, r, s, t, то

$$(h, k) = (k, h) = L_m \cap L_n.$$

Легко проверить, что (h, k), (k, m), (m, h) будут тремя попарно различными точками прямой L_n и что, следовательно,

$$(1) \qquad L_n = (h, k) + (k, m) = (k, m) + (m, h) = (m, h) + (h, k).$$



Фиг. 14.

Построенный основной четырехугольник мы зафиксируем на время всего нашего рассмотрения. Через x, y, z мы будем обозначать любые три различных из четырех символов o, r, s, t.

Теперь мы построим

Векторы (*относительно основного четырехугольника* L_o, L_r, L_s, L_t).

$v = [v_o, v_r, v_s, v_t]$ является вектором с x-координатой v_x, если каждая координата v_x представляет собой такой элемент множества S, что

$$(2.а) \qquad r(v_x) \leqslant 1,$$

$$(2.б) \qquad v_x + (x, y) = (x, y) + v_y = v_y + v_x \text{ для } x \neq y.$$

Приведенное нами построение векторов очень похоже на построение, принадлежащее Гессенбергу, который руководствовался построениями, обычными в дескриптивной геометрии. Наше понятие вектора станет более наглядным, если рассмотреть его в системе $S(F, A)$ подпространств F-пространства A. Для этого

выберем три линейно независимых элемента r, s, t F-пространства A и положим

$$L_o = F(r-s)+F(s-t)+F(t-r),$$
$$L_r = Fs+Ft,\quad L_s = Ft+Fr,\quad L_t = Fr+Fs;$$

$(x, y) = F(x-y)$ для любых двух различных x, y из четырех символов o, r, s, t [здесь мы полагаем $o = 0$].

Очевидно, что эти прямые L_o, L_r, L_s, L_t образуют основной четырехугольник рассматриваемого вида.

Если a — элемент F-пространства A, то

$$v(a) = [Fa,\ F(a-r),\ F(a-s),\ F(a-t)]$$

будет вектором, x-координата которого совпадает с $F(a-x)$; читатель может проверить, что в рассматриваемом случае каждый вектор определяется указанным образом одним и только одним элементом из A. Эту иллюстрацию следует иметь в виду на протяжении всего нашего последующего рассмотрения. Некоторые из проводимых здесь построений для случая, когда S есть система подпространств F-пространства A, читатель может найти в добавлении I к гл. III.

Возвратимся теперь к нашему изучению векторов над основным четырехугольником L_o, L_r, L_s, L_t. Если x — один из символов o, r, s, t, то определим следующим образом вектор, который также будем обозначать через x:

$$x_y = \begin{cases} 0 & \text{для } x = y, \\ (x, y) & \text{для } x \neq y. \end{cases} \tag{3}$$

Из свойства (2.б) легко следует, что если, обратно, координата v_x вектора v равна 0, то $v = x$. Заметим, что самое большее одна координата вектора может быть равна 0, что все отличные от 0 координаты являются точками и что лишь построенные сейчас специальные векторы x имеют одну нулевую координату.

(4) *Произвольный вектор имеет самое большее две одинаковые координаты; из* $v_x = v_y$ *для* $x \neq y$ *следует* $v_x = v_y = (x, y)$.

Доказательство. Если $v_x = v_y$ при $x \neq y$, то, в силу сделанного выше замечания, ни одна из координат вектора v не равна 0, а из свойства (2.б) вытекает, что $(x, y) \leqslant v_x$. Но так как и v_x и (x, y) являются точками, то, следовательно, $v_x = (x, y)$. Если бы, кроме того, имело место равенство $v_x = v_z$, то мы подобным же образом показали бы, что $v_x = (x, z)$; но тогда мы бы имели $(x, y) = (x, z)$, а это несовместимо с неравенством $y \neq z$. Пусть, наконец, при некоторой перестановке h, k, m, n символов o, r, s, t справедливы равенства $v_h = v_k$ и $v_m = v_n$; в таком случае $v_h = v_k = (h, k)$ и $v_m = v_n = (m, n)$. Но отсюда и из свойства (2.б) следует, что $(h, m) \leqslant v_h + v_m = (h, k) + (m, n)$, а это противо-

речит свойствам основного четырехугольника. Таким образом, вектор v имеет самое большее две одинаковые координаты.

Предложение 1. *Если P и Q — такие различные точки множества S, что*

$$P + Q = P + (x, y) = (x, y) + Q,$$

то существует, и притом только один, такой вектор v, что $v_x = P$, $v_y = Q$.

Доказательство. Предположим сначала, что существуют два вектора v и w, удовлетворяющие условиям $P = v_x = w_x$, $Q = v_y = w_y$. Оставшуюся пару индексов обозначим через h, k. Если z — отличный от x и y индекс, то, по свойству (2.б),

$$v_z + w_z \leqslant [P + (x, z)] \cap [Q + (y, z)].$$

Допустим, что $v_z \neq w_z$. Если бы координата v_z равнялась 0, то было бы $v = z$ и, следовательно, $P = (x, z)$, $Q = (y, z)$. Но отсюда вытекало бы, что $w_z = 0$, а это противоречит нашему предположению о том, что $v_z \neq w_z$. Из тех же соображений видно, что и $w_z \neq 0$; следовательно, v_z и w_z являются точками. Но тогда из полученного выше включения, принимая во внимание, что $P \neq Q$, легко вывести, что

$$v_z + w_z = P + (x, z) = Q + (y, z) = P + Q = (x, z) + (z, y).$$

Если бы одновременно имели место неравенства $v_h \neq w_h$ и $v_k \neq w_k$, то из результата предыдущего абзаца следовало бы, что

$$L_k = (x, h) + (h, y) = v_h + w_h = P + Q = v_k + w_k = (x, k) + (y, k) = L_h;$$

но, поскольку $h \neq k$, полученное равенство противоречит свойствам основного четырехугольника. Таким образом, можно предположить, что $v_h = w_h$. Тогда, в силу свойства (2.б), мы имеем

$$v_k + w_k \leqslant [v_h + (h, k)] \cap [P + (x, k)] \cap [Q + (y, k)].$$

Отсюда, если бы было $v_k \neq w_k$, мы так же, как и выше, получили бы, что

$$v_k + w_k = v_h + (h, k) = P + (x, k) = Q + (y, k) = P + Q = \\ = (h, k) + (x, k) = (x, k) + (y, k),$$

и вновь пришли бы к противоречию со свойствами основного четырехугольника. Следовательно, $v_k = w_k$, и этим полностью доказано, что $v = w$. Таким образом, если существует вектор, обладающий требуемыми свойствами, то он определяется однозначно.

При построении такого вектора мы будем различать два возможных случая.

Случай 1: по крайней мере одна из точек P, Q лежит хотя бы на одной из прямых $(x, h)+(h, y)$ и $(x, k)+(k, y)$. Без ограничения общности можно предположить, что на прямой $(x, h)+(h, y)$ лежит точка P. Поскольку эта прямая проходит через точку (x, y) и так как $P+(x, y)=P+Q$ является прямой, то

$$P+Q=(x, h)+(h, y)=L_h.$$

Если хотя бы одна из точек P, Q лежала бы и на прямой $(x, k)+(k, y)$, то мы подобным же образом вывели бы, что $P+Q=(x, k)+(k, y)$; отсюда следовало бы совпадение прямых L_k и L_h, что невозможно. Таким образом, ни точка P, ни точка Q не лежат на прямой $(x, k)+(k, y)$. Но в таком случае $P+(x, k)$ и $Q+(k, y)$ будут двумя различными прямыми, лежащими в одной плоскости

$$P+Q+(x, k)+(k, y)=P+(x, y)+(x, k)+(k, y)=$$
$$=P+(x, k)+(k, y).$$

Различные же прямые, лежащие в одной плоскости, пересекаются по точке; следовательно,

$$K=[P+(x, k)]\cap[Q+(k, y)]$$

является вполне определенной точкой. Если бы точка K совпала с P, то $Q+(k, y)$ совпала бы с $P+Q=(x, h)+(h, y)$, что невозможно; также невозможно, чтобы точка K совпала с точкой (x, k), ибо отсюда следовало бы совпадение прямых $Q+(k, y)$ и

$$(x, k)+(k, y)=Q+(x, y)=P+Q=(x, h)+(h, y).$$

Аналогично доказывается, что точка K отлична от точек Q и (k, y). Поэтому

$$P+(x, k)=(x, k)+K=K+P,\quad Q+(y, k)=(y, k)+K=K+Q.$$

и $K+P$ и $K+Q$ являются прямыми. Если бы точка K лежала на прямой $P+Q$, то с этой прямой совпадали бы прямые $K+P$ и $K+Q$ и, следовательно, прямая $P+Q=(x, h)+(h, y)$ проходила бы через точки (x, k) и (k, y), что невозможно. Таким образом, K не содержится в $P+Q$.

Если $K=(h, k)$, то

$$P=[(x, h)+(h, y)]\cap[(x, k)+(k, h)]=(x, h),$$
$$Q=[(x, h)+(h, y)]\cap[(y, k)+(k, h)]=(y, h),$$

и h будет требуемым вектором.

Если же $K\neq(h, k)$, то мы так же, как выше, можем показать, что $H=[P+Q]\cap[K+(h, k)]$ является точкой. Так как ни одна из точек K и (h, k) не лежит на прямой $P+Q=(x, h)+$

$+(y, h)$, то точка H отлична от K и (h, k); следовательно,

$$K+(h, k)=(h, k)+H=H+K.$$

Если $H=P$, то $H+K=P+K=(x, k)+(h, k)$, так что $P=(x, h)$. Но в таком случае, полагая

$$v_x=P=(x, h),\quad v_y=Q,\quad v_h=(x, h),\quad v_k=K,$$

мы, как легко проверить, получим вектор v, удовлетворяющий нашим условиям. Подобным же образом мы найдем нужный нам вектор в случае, когда $H=Q$. Если, наконец, точка H отлична от точек P и Q, то

$$P+Q=Q+H=H+P=H+(x, h)=(y, h)+H,$$

так как, например, из $H=(x, h)$ следовало бы, что прямая $H+K$ проходит через точку (x, k) и поэтому $H+K=H+P=P+Q$, что невозможно. Ввиду полученного равенства, вектор v, координатами которого служат

$$v_x=P,\quad v_y=Q,\quad v_k=K,\quad v_h=H,$$

удовлетворяет нашим требованиям.

Случай 2: ни одна из точек P и Q не лежит на прямых $(x, h)+(h, y)$ и $(x, k)+(k, y)$ (фиг. 15). В этом случае $P+(x, z)$ и $Q+(y, z)$ для $z=h, k$ будут различными прямыми, пересекающимися в точке $Z=[P+(z, x)]\cap[Q+(z, y)]$. Легко проверить, что точка Z отлична от точек P, (z, x), Q, (z, y); поэтому

$$P+(z, x)=(z, x)+Z=Z+P,\ Q+(z, y)=(z, y)+Z=Z+Q$$

для $z=h, k$.

Естественно, что прямая $P+Q$ отлична от прямых $(x, h)+(h, y)$ и $(x, k)+(k, y)$. Таким образом, треугольники P, (x, h), (x, k) и Q, (y, h), (y, k) перспективны, с центром перспективы в точке $(x; y)$ [здесь мы используем наше предположение о коллинеарности точек P, Q, (x, y)], и выполняются все условия теоремы Дезарга (аксиомы IX). Но соответствующие стороны наших двух треугольников пересекаются в точках

$$[P+(x, h)]\cap[Q+(y, h)]=H,\quad [P+(x, k)]\cap[Q+(y, k)]=K,$$

$$[(x, h)+(x, k)]\cap[(y, h)+(y, k)]=(h, k);$$

следовательно, по теореме Дезарга, $H+K=K+(h, k)=(h, k)+H$. Поэтому вектор v, удовлетворяющий нашим требованиям, определяется следующим образом:

$$v_x=P,\quad v_y=Q,\quad v_h=H,\quad v_k=K;$$

этим предложение 1 полностью доказано.

В дальнейшем мы всюду будем пользоваться следующим *обозначением: если v и w — векторы, то*

$$(v+w)^* = (v_0+w_0) \cap (v_r+w_r) \cap (v_s+w_s) \cap (v_t+w_t).$$

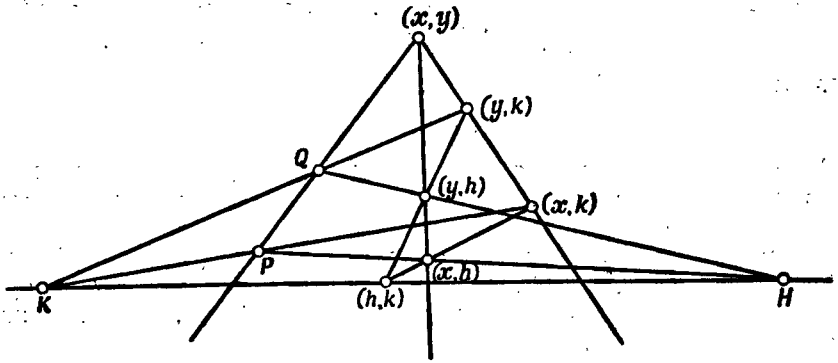
Таким образом, $(v+w)^*$ является вполне определенным элементом множества S.

Предложение 2. (а) $r[(v+w)^*] \leqslant 1$.

(б) $(v+w)^* = 0$ *тогда и только тогда, когда* $v = w$.

(в) $(v+w)^* + v_x = (v+w)^* + w_x$ *для каждого* x.

Доказательство. Так как $(v+w)^* \leqslant v_x + w_x$, то ясно, что $r[(v+w)^*] \leqslant 2$. Если бы ранг элемента $(v+w)^*$ был равен 2,



Фиг. 15.

то имело бы место равенство $(v+w)^* = v_x + w_x$ для каждого x; отсюда, в частности, следовало бы, что $(x, y) \leqslant v_x + v_y \leqslant (v+w)^*$ для $x \neq y$. Но сумма всех точек (x, y) имеет ранг 3; таким образом, мы пришли к противоречию, чем и доказана справедливость утверждения (а).

Если $v = w$, то $(v+w)^* = v_0 \cap v_r \cap v_s \cap v_t$. Поскольку ранг каждой координаты вектора не превышает 1 и так как, в силу утверждения (4), вектор имеет самое большее две одинаковые координаты, то, следовательно, из $v = w$ вытекает, что $(v+w)^* = 0$.

Докажем теперь, что

(5) $(v+x)^* = v_x$ *для каждого индекса* x *и каждого вектора* v.

Это утверждение становится очевидным, если принять во внимание, что $v_y + x_y = v_y + (x, y) = v_y + v_x$ для $x \neq y$ и что $v_x + x_x = v_x$.

Предположим теперь, что для некоторого индекса x

$$(v+w)^* + v_x \neq (v+w)^* + w_x.$$

Тогда $v_x \neq w_x$. Если $(v+w)^* = v_x$, то v_x содержится в $v_y + w_y$ для каждого $y \neq x$. Отсюда и из включения $(x, y) \leqslant v_x + v_y$

следует, что $(x, y) \leqslant v_y + w_y$; принимая теперь во внимание равенство $(x, y) + w_y = w_x + w_y$, мы получаем, что $w_x \leqslant v_y + w_y$ для каждого x. Таким образом, $w_x \leqslant (v+w)^* = v_x$; так как $w_x \neq v_x$ и ранг координаты v_x не превышает 1, то из последнего соотношения вытекает, что $w_x = 0$. Но тогда

$$(v+w)^* + v_x = v_x = (v+w)^* + w_x,$$

что противоречит нашему предположению. Из тех же соображений видно, что $(v+w)^* \neq w_x$. Но

$$(v+w)^* \leqslant v_x + w_x;$$

поэтому, если бы элемент $(v+w)^*$ был отличен и от 0, то было бы

$$v_x + w_x = w_x + (v+w)^* = (v+w)^* + v_x,$$

что невозможно. Следовательно,

$$(v+w)^* = 0.$$

[Заметим, что из определения (3) и утверждения (5) вытекает, что координаты v_x и w_x не могут быть равны 0; таким образом, v_x и w_x являются точками, а $v_x + w_x$ — прямой.]

Если $v_y = 0$, то $v = y$ и, в силу утверждения (5), $(v+w)^* = w_y$. Отсюда вытекает, что $w_y = 0$ и $w = y$. Но тогда $v = w$, что противоречит неравенству $v_x \neq w_x$; следовательно, v_y, так же как и w_y, отлично от 0.

Предположим теперь, что $v_y = w_y$ и $v_z = w_z$ для $y \neq z$. Тогда, поскольку $v \neq w$, из предложения 1 следует, что $v_y = v_z = w_y = w_z = (y, z)$. Если u — отличный от y и z индекс, то, вновь пользуясь тем, что $v \neq w$, и предложением 1, мы получаем, что $v_u \neq w_u$. Поэтому

$$v_u + (u, y) = v_u + v_y = v_u + (y, z) = (u, y) + (y, z) = w_u + (u, y) = v_u + w_u$$

и, следовательно, $(y, z) = (v+w)^* = 0$, что невозможно.

Пусть теперь $v_y = w_y$ для некоторого y. В таком случае, как следует из результата, полученного в предыдущем абзаце, v_z и w_z будут различными точками для каждого $z \neq y$. Следовательно,

$$v_z + (y, z) = (y, z) + v_y = (y, z) + w_y = w_z + (y, z) = v_z + w_z,$$

так что $v_y = w_y \leqslant v_z + w_z$ для каждого z и поэтому $0 \neq v_y \leqslant (v+w)^* = 0$, что невозможно. Таким образом, мы показали, что

v_y и w_y являются различными точками для каждого индекса y.

Рассмотрим теперь прямые $v_o + w_o$, $v_r + w_r$, $v_s + w_s$ и $v_t + w_t$. Любые две из них расположены в одной плоскости, ибо

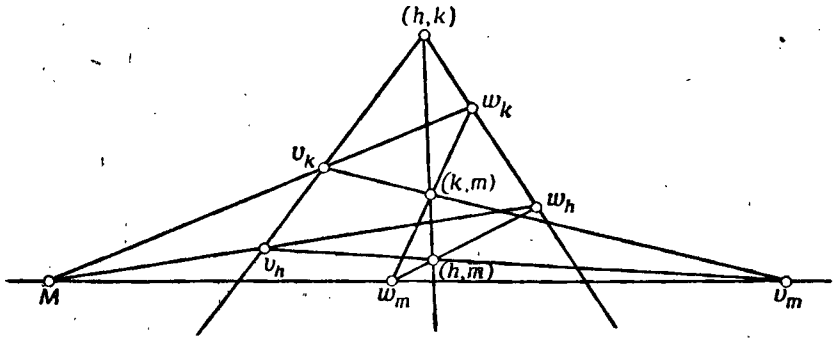
$$v_x + w_x + v_y + w_y = u_x + (x, y) + w_x.$$

Таким образом, любые две из этих прямых либо совпадают, либо имеют одну общую точку. Если бы среди этих прямых были только две различные, то точка их пересечения совпадала бы с $(v+w)^*=0$, что невозможно. Следовательно,

по крайней мере три из прямых v_x+w_x *попарно различны.*

Докажем теперь следующие утверждения.

(г) *Если* $v_h+w_h\neq v_k+w_k$, *то* v_h, v_k, (h, k) *будут тремя попарно различными точками.*



Фиг. 16.

Действительно, в силу свойства (2.б), из совпадения каких-либо двух из трех точек v_h, v_k, (h, k) следует, что все три точки совпадают между собой. Если же $v_h=v_k=(h, k)$, то, по свойству (2.б), $v_h+w_h=(h, k)+w_h=w_k+(h, k)=w_k+v_k$; этим утверждение (г) доказано.

(д) *Если* v_h+w_h, v_k+w_k, v_m+w_m — *три попарно различные прямые и если ни* $v_h+v_k+v_m$, *ни* $w_h+w_k+w_m$ *не является прямой, то*

$$(v_h+w_h)\bigcap(v_k+w_k)\bigcap(v_m+w_m)\ \textit{будет точкой.}$$

Из наших предположений следует, что $(v_h+w_h)\bigcap(v_k+w_k)=M$ является точкой; таким образом, нам нужно только показать, что точка M лежит на прямой v_m+w_m (фиг. 16). В силу утверждения (г), $v_h\neq v_k$; отсюда и из наших предположений вытекает, что $r(v_h+v_k+v_m)=3$; из тех же соображений видно, что $r(w_h+w_k+w_m)=3$.

Заметим теперь, что треугольники v_h, w_h, (h, m) и v_k, w_k, (k, m) перспективны с центром перспективы в точке (h, k), которая отлична от всех вершин этих треугольников. Прямые v_h+v_k и w_h+w_k различны, ибо в противном случае мы имели бы $v_h+w_h=v_k+w_k=v_h+v_k=w_h+w_k$. Прямая v_h+v_k отлична от прямой $(h, m)+(k, m)$, так как иначе на прямой v_h+v_k лежала бы точка v_m; подобным же образом, $w_h+w_k\neq(h, m)+(k, m)$.

Прямые $v_h + w_h$ и $v_k + w_k$ пересекаются в точке M. Поскольку ранг $r(v_h + v_k + v_n) = 3$, не могут совпасть друг с другом прямые $v_h + (m, h)$ $v_h + v_m$ и $v_k + (m, k) = v_k + v_m$.
Следовательно,

$$[v_h + (m, h)] \cap [v_k + (m, k)] = v_m.$$

Аналогично,

$$[w_h + (m, h)] \cap [w_k + (m, k)] = w_m.$$

Таким образом, мы проверили справедливость всех условий теоремы Дезарга (аксиомы IX). В силу этой теоремы, точки M, v_n, w_m коллинеарны, что и требовалось доказать.

(д'). *Ни для какой тройки индексов h, k, m предположения утверждения* (д) *не выполняются.*

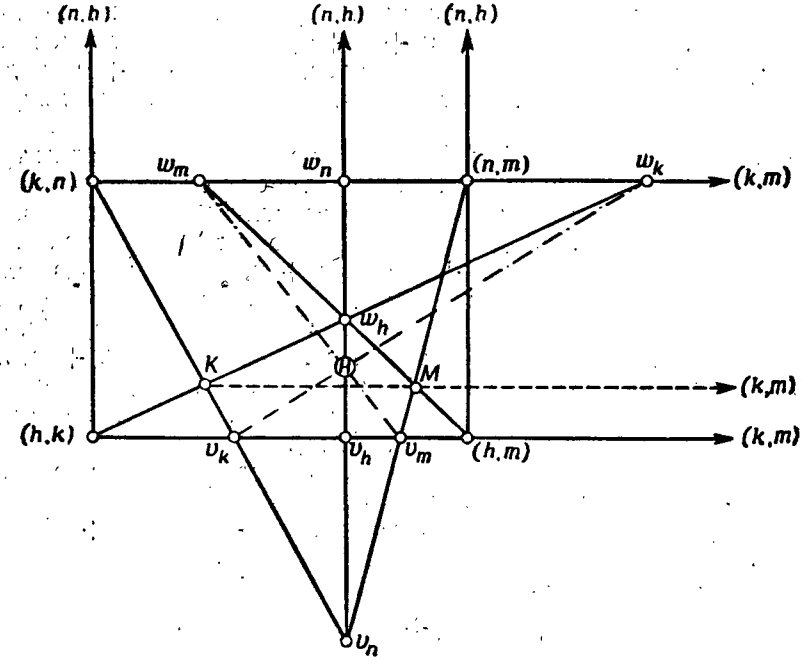
Действительно, пусть предположения утверждения (д) справедливы для тройки индексов h, k, m. Тогда $N = (v_h + w_h) \cap (v_k + w_k) \cap (v_m + w_m)$ будет точкой. Если бы прямая $v_n + w_n$ совпадала с одной из прямых $v_z + w_z$, $z = h, k, m$, то точка N лежала бы и на прямой $v_n + w_n$ и, следовательно, $0 = (v + w)^* = N$ был бы точкой, что невозможно. Таким образом, прямая $v_n + w_n$ отлична от всех прямых $v_z + w_z$, где $z = h, k, m$. Отсюда и из утверждения (г) вытекает, что v_o, v_r, v_s, v_t представляют собой четыре попарно различные точки; в силу тех же соображений, четырьмя попарно различными точками будут w_o, w_r, w_s, w_t. Поэтому точка v_n лежит самое большее на одной из трех прямых $v_h + v_k$, $v_k + v_m$, $v_m + v_h$ (эти прямые попарно различны, поскольку точки v_h, v_k, v_m, по предположению, порождают плоскость); аналогичное утверждение справедливо и для точки w_n. Следовательно, существуют такие два из трех индексов h, k, m (их мы обозначим через a, b), что точка v_n не лежит на прямой $v_a + v_b$, а точка w_n не лежит на прямой $w_a + w_b$. Тогда не будут прямыми ни $v_n + v_a + v_b$, ни $w_n + w_a + w_b$; в то же время $v_n + w_n$, $v_a + w_a$, $v_b + w_b$ являются тремя попарно различными прямыми. Поэтому можно воспользоваться утверждением (д), в силу которого $N' = (v_n + w_n) \cap (v_a + w_a) \cap (v_b + w_b)$ будет точкой. С другой стороны, поскольку прямые $v_a + w_a$ и $v_b + w_b$ различны и так как a, b являются двумя из трех индексов h, k, m, то $N' = (v_a + w_a) \cap (v_b + w_b) = N$. Отсюда следует, что $0 = (v + w)^* = N = N'$; полученное противоречие доказывает справедливость утверждения (д').

(е) *Все четыре прямые $v_z + w_z$, $z = o, r, s, t$, не могут быть различными.*

Действительно, пусть все четыре прямые попарно различны. Тогда, в силу утверждения (д'), либо $v_h + v_k + v_m$, либо $w_h + w_k + w_m$ будет прямой для каждой тройки индексов h, k, m. Если $v_h + v_k + v_m$ является прямой, то эта прямая совпадает с прямой $(h, k) + (k, m)$. Если бы и $w_h + w_k + w_m$ была прямой, то и она

совпадала бы с прямой $(h, k)+(k, m)$. Но отсюда следовало бы, что $v_h+w_h=v_k+w_k=(h, k)+(k, m)$, что невозможно. Тем самым мы показали, что если h, k, m — произвольная тройка индексов, то один и только один из элементов $v_h+v_k+v_m$ и $w_h+w_k+w_m$ представляет собой прямую, а другой будет плоскостью.

Без ограничения общности можно предположить, что $v_0+v_r+v_s$ является прямой, а $w_0+w_r+w_s$—плоскостью. Так как $v_0+v_r+v_s+v_t$,



Фиг. 17.

в силу свойства (2.б), содержит плоскость, порожденную всеми точками (h, k), то невозможно, чтобы точка v_t лежала на прямой $v_0+v_r+v_s$. Поэтому $v_0+v_r+v_t$ не будет прямой; но тогда, в силу результата предыдущего абзаца, элемент $w_0+w_r+w_t$ представляет собой прямую. Из тех же соображений видно, что прямыми являются также $w_r+w_s+w_t$ и $w_s+w_0+w_t$. Из утверждения же (г) вытекает, что все точки w_0, w_r, w_s, w_t попарно различны. Поэтому точки w_0 и w_s лежат на прямой w_r+w_t, и, следовательно, $w_0+w_r+w_s+w_t$ является прямой. Но это приводит нас к противоречию с тем, что $w_0+w_r+w_s$ является плоскостью; полученное противоречие доказывает справедливость утверждения (е).

Из утверждения (е) следует, что при должном выборе обозначений прямые w_h+v_h, w_k+v_k, w_n+v_n будут попарно различными, а прямая w_n+v_n совпадает с прямой w_h+v_h. В силу утверждения (д'), один из элементов $v_h+v_k+v_m$ и $w_h+w_k+w_m$ представляет собой прямую, а другой плоскость; без ограничения общности можно предположить, что $v_h+v_k+v_m$ является прямой, а $w_h+w_k+w_m$ — плоскостью.

Так как сумма всех четырех точек v_z содержит плоскость, порождаемую всеми (i, j), то точка v_n не лежит на прямой $v_h+v_k+v_m$. Следовательно, $v_k+v_n+v_n$ является плоскостью; отсюда и из утверждения (д') вытекает, что $w_k+w_n+w_n$ будет прямой; эта прямая не может содержать точку w_h. Рассмотрим теперь два случая.

Случай 1: $v_n \neq w_h$ (фиг. 17). В этом случае перспективны треугольники w_h, (h, k), (h, m) и v_n, (k, n), (n, m) с центром перспективы в точке (n, h); при этом три прямые, соединяющие перспективные вершины наших треугольников, попарно различны, так как если бы, например, было $w_h+v_n=(h, k)+(k, n)$, то отсюда следовала бы коллинеарность точек w_h, w_k, w_n. Прямые $w_h+(h, k)$ и $v_n+(k, n)$ различны и пересекаются в точке K; прямые $w_h+(h, m)$ и $v_n+(n, m)$ пересекаются в точке M; прямые же $(h, k)+(h, m)$ и $(k, n)+(n, m)$ пересекаются в точке (k, m). Следовательно, мы можем воспользоваться теоремой Дезарга, из которой вытекает коллинеарность точек M, K, (k, m).

Треугольники M, w_m, v_m и K, w_k, v_k перспективны с центром перспективы в точке (k, m); соответствующие стороны этих треугольников пересекаются в точках $[w_m+v_n]\cap[w_k+v_k]=H$, v_n, w_h. Легко проверить, что и здесь применима теорема Дезарга. Поэтому точка H лежит и на прямой

$$v_n+w_h=v_n+w_n=v_h+w_h,$$

и этим показано, что $0=(v+w)^*=H$; тем самым мы пришли к противоречию.

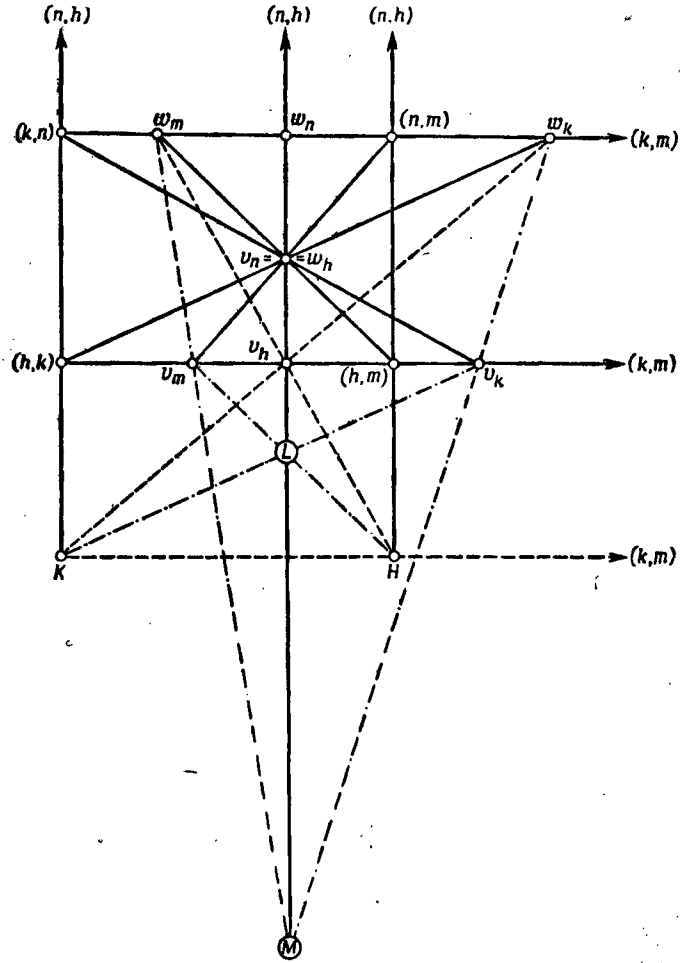
Случай 2: $v_n=w_h$ (фиг. 18). В этом случае, чтобы прийти к нужному нам результату, теоремой Дезарга придется воспользоваться трижды. Треугольники w_k, v_h, w_m и (h, k), (n, h), (h, m) перспективны с центром перспективы в точке $v_n=w_h$; точками пересечения соответствующих сторон этих треугольников будут

$$H=[v_h+w_m]\cap[(n, h)+(h, m)],\ (k, m) \text{ и } K=[w_k+v_h]\cap[(h, k)+(n, h)].$$

Легко проверить, что здесь можно применить теорему Дезарга, из которой следует коллинеарность точек H, K, (k, m).

Треугольники H, v_m, (m, k) и (n, h), v_n, (n, k) перспективны с центром перспективы в точке (m, n); точками пересечения соответствующих сторон этих треугольников будут v_k, K и $L=[v_m+H]\cap[v_n+(n, h)]$. Здесь также можно воспользоваться

теоремой Дезарга, из которой мы получаем, что L является точкой пересечения трех прямых $K+v_h$, $H+v_m$ и $v_n+(n,\ h)=$ $=v_n+v_h=w_h+v_h$.



Фиг. 18.

Треугольники H, v_m, w_m и K, v_k, w_k перспективны с центром перспективы в точке $(k,\ m)$, ибо, как мы показали в начале рассмотрения случая 2, точки H, K, $(k,\ m)$ коллинеарны. Из результата предыдущего абзаца и из построения точек H и K вытекает, что точками пересечения соответствующих сторон

наших треугольников будут

$$[H+v_m]\cap[K+v_k]=L,\quad [H+w_m]\cap[K+w_k]=v_h,$$
$$[v_m+w_m]\cap[v_k+w_k]=M.$$

Мы уже отмечали, что точка L лежит на прямой w_h+v_h, причем, так как $L\neq v_h$, то $w_h+v_h=L+v_h$. Отсюда, используя теорему Дезарга, мы получаем, что точка M лежит и на прямой w_h+v_h. Следовательно, $0=(v+w)^*=M$. Таким образом, мы вновь пришли к противоречию, и этим завершается доказательство утверждения (в).

Из утверждения (в) и из того, что было показано в начале нашего доказательства, непосредственно следует справедливость утверждения (б). Таким образом, предложение 2 полностью доказано.

Следствие 1. *Если v и w — векторы, то*

$$v_x+w_x=w_x+(v+w)^*=(v+w)^*+v_x \text{ для каждого } x.$$

Доказательство. Если $v=w$, то наше утверждение тривиально, ибо в этом случае, в силу предложения 2 (б), $(v+w)^*=0$. Если же $v\neq w$, то, как следует из предложения 2, $(v+w)^*$ будет точкой. В случае, когда $v_x=0$, вектор v совпадает с вектором x и поэтому $w_x\neq 0$; в силу же утверждения (5), в этом случае $(v+w)^*=w_x$. Если и v_x и w_x отличны от 0, то справедливость нашего утверждения вытекает из предложения 2 (в); при этом нужно принять во внимание, что из $v_x=w_x$ следует $v_x=w_x=(v+w)^*$, ибо $(v+w)^*\leqslant v_x+w_x$.

Предложение 3. *Для каждого вектора v и любой пары различных точек P и Q, удовлетворяющих условию $P+Q=v_x+P$, существует, и притом только один, такой вектор w, что $P=(v+w)^*$ и $Q=w_x$.*

Доказательство. Предположим сначала, что существуют два вектора w' и w'', удовлетворяющие условиям

$$P=(v+w')^*=(v+w'')^* \text{ и } Q=w'_x=w''_x.$$

Так как ранг суммы координат вектора v не меньше 3 [эта сумма содержит плоскость, порождаемую всеми точками (x, y)], то существует такой индекс y, что координата v_y является точкой, не лежащей на прямой $P+Q$. Если бы точка Q совпадала с точкой (x, y), то мы имели бы либо $Q=v_x=v_y=(x, y)$, либо $P+Q=Q+v_x=(x, y)+v_x=v_x+v_y$. Но оба соотношения противоречат выбору индекса y [1]). Таким образом, $Q\neq(x, y)$. Далее, в силу следствия 1,

$$v_y+w'_y=w'_y+P=P+v_y,$$

[1]) Первое равенство невозможно и в силу основного предположения. — *Прим. перев.*

а из свойства (2.б) вытекает, что

$$Q+w'_y=w'_y+(x, y)=(x, y)+Q.$$

Поскольку точки P и v_y различны, $P+v_y$ является прямой. Как было показано выше, также различны точки Q и (x, y); следовательно, и $Q+(x, y)$ будет прямой. Эти прямые различны, ибо в противном случае точка v_y лежала бы на прямой $P+Q$ (с этой прямой совпали бы обе рассматриваемые прямые в случае их совпадения между собой). В то же время и прямая $P+v_y$, и прямая $Q+(x, y)$ проходят через точку w'_y; следовательно, $[P+v_y]\cap[Q+(x, y)]=w'_y$. Но подобным же образом можно показать, что $[P+v_y]\cap[Q+(x, y)]=w''_y$. Таким образом, $w'_x=Q=w''_x$ и $w'_y=w''_y$ для некоторого $y\neq x$. Поскольку $Q\neq(x, y)$, то, в силу утверждения (4), x- и y-координаты как вектора w', так и вектора w'' различны; отсюда и из предложения 1 следует, что $w'=w''$. Тем самым показано, что существует самое большее один вектор, удовлетворяющий нашим требованиям.

Для доказательства существования требуемого вектора w мы используем тот же метод, каким пользовались при предыдущем рассмотрении. Сначала выберем такой индекс y, что v_y является точкой, не лежащей на прямой $P+Q$; это сделать можно, поскольку ранг суммы координат вектора v не меньше 3. Точно так же, как это было сделано выше, можно показать, что $Q\neq(x, y)$ и что $P+v_y$ и $Q+(x, y)$ являются двумя различными прямыми, пересекающимися в точке $M=[P+v_y]\cap[Q+(x, y)]$. Если хотя бы одна из точек Q и (x, y) лежала бы на прямой $P+v_y$, то эта прямая совпала бы с прямой $P+Q$, ибо

$$(x, y)+v_y=v_x+(x, y)=v_x+P=P+Q,$$

что невозможно; из тех же соображений видно, что ни точка P, ни точка v_y не лежат на прямой $Q+(x, y)$. Следовательно, точка M отлична от точек P, Q, v_y и (x, y); отсюда вытекает, что $Q+(x, y)=(x, y)+M=M+Q$. Теперь воспользуемся предложением 1, из которого следует существование одного и только одного такого вектора w, что $w_x=Q$ и $w_y=M$. Так как $w_y=M\neq v_y$, то $w\neq v$; отсюда и из предложения 2 вытекает, что $(v+w)^*$ будет точкой. Эта точка лежит на прямых $v_x+w_x=v_x+Q=P+Q$ и $v_y+w_y=v_y+M=P+v_y$, которые различны, поскольку точка v_y не лежит на прямой $P+Q$. Но общей точкой этих двух прямых является точка P; следовательно, $P=(v+w)^*$. Таким образом, вектор w удовлетворяет всем нашим требованиям.

Замечание 1. Если v — вектор и P — произвольная точка, то по крайней мере одна из координат вектора v, например v_x, будет точкой, отличной от P (здесь мы пользуемся тем, что

ранг суммы координат данного вектора не меньше 3). По аксиоме VIII, прямая $P+v_x$ содержит по крайней мере еще одну точку Q. Таким образом, $P+v_x=v_x+Q=P+Q$; отсюда и из предложения 3 вытекает существование такого вектора w, что $P=(v+w)^*$ и $Q=w_x$. Векторы v и w непременно различны, поскольку $v_x \neq w_x$; в то же время, в силу следствия 1,

$$v_z+w_z=w_z+P=P+v_z$$

для каждого индекса z.

Предложение 4. *Если u, v, w — три попарно различных вектора, то либо*

$$(u+v)^*=(v+w)^*=(w+u)^*,$$

либо

$$(u+v)^*,\ (v+w)^*,\ (w+u)^*$$

будут тремя попарно различными коллинеарными точками.

Доказательство. Предположим сначала, что $(u+v)^*=(v+w)^*$. Тогда, в силу следствия 1,

$$u_x+v_x=v_x+(u+v)^*=v_x+(v+w)^*=v_x+w_x \text{ для каждого } x$$

и

$$u_x+w_x=w_x+(u+w)^*=(u+w)^*+u_x \text{ для каждого } x.$$

Если $u_x=0$, то $u=x$ и $(u+w)^*=w_x$; подобным же образом из $w_x=0$ вытекает, что $(u+w)^*=u_x$. Если $u_x=w_x\neq 0$, то $(u+w)^*=u_x=w_x$, ибо, в силу предложения 2, $(u+w)^*$ является точкой. Если, наконец, u_x и w_x — различные точки, то прямая $u_x+v_x=v_x+w_x=w_x+u_x$ проходит через $(u+w)^*$. Таким образом, мы показали, что во всех случаях

$$(u+w)^*\leqslant u_x+v_x=v_x+w_x \text{ для каждого } x;$$

отсюда вытекает, что $(u+w)^*\leqslant(u+v)^*=(v+w)^*$. Но в силу предложения 2, $(u+w)^*$ и $(u+v)^*$ являются точками; ввиду полученного включения эти точки совпадают.

Из предложения 2 вытекает, что $(u+v)^*$, $(v+w)^*$ и $(w+u)^*$ являются точками; как только что было показано, либо все эти точки совпадают, либо они попарно различны. Таким образом, мы можем теперь предположить, что $(u+v)^*$, $(v+w)^*$ и $(w+u)^*$ — три попарно различные точки. Если существует такой индекс x, что $r(u_x+v_x+w_x)<3$, то коллинеарность трех точек $(u+v)^*$, $(v+w)^*$, $(w+u)^*$ будет следовать из включения

$$(u+v)^*+(v+w)^*+(w+u)^*\leqslant u_x+v_x+w_x.$$

Следовательно, мы можем теперь предположить, что

$$r(u_x+v_x+w_x)=3 \text{ для каждого } x. \qquad (*)$$

Отсюда, в частности, вытекает, что u_x, v_x, w_x являются точками и что для каждого x прямые u_x+v_x, v_x+w_x и w_x+u_x попарно различны.

В силу утверждения (4), самое большее две координаты вектора совпадают между собой. Таким образом, существует самое большее одна такая пара индексов x_0, y_0, что $w_{x_0}=w_{y_0}$. Если бы прямые u_x+v_x и u_y+v_y совпадали для каждой такой пары индексов $x\neq y$, что $w_x\neq w_y$, то мы имели бы

$$u_o+v_o=u_r+v_r=u_s+v_s=u_t+v_t$$

и ранг суммы координат вектора u (а также вектора v) был бы меньше 3, что невозможно, поскольку сумма координат произвольного вектора содержит сумму всех точек (h, k), ранг которой равен 3. Следовательно, существует такая пара индексов x, y, что

$$u_x+v_x\neq u_y+v_y \text{ и } w_x\neq w_y.$$

Так как u_x+v_x и u_y+v_y — различные прямые, то ранг их суммы не меньше 3. Если бы было $v_x\leqslant u_x+u_y$, то мы имели бы

$$u_x+u_y=u_x+u_y+v_x=u_x+u_y+(x, y)+v_x=u_x+u_y+v_y+v_x,$$

и, следовательно, эта сумма имела бы ранг 2. Но это невозможно; таким образом, мы показали, что точка v_x не лежит на u_x+u_y. Из тех же соображений видно, что на u_x+u_y не лежит и точка v_y. Если бы совпадали между собой точки v_x и v_y, то, в силу утверждения (4), обе эти точки совпали бы с точкой (x, y) и поэтому лежали бы на u_x+u_y; следовательно, v_x+v_y является прямой. Подобным же образом можно показать, что u_x+u_y также является прямой и что прямые u_x+u_y и v_x+v_y различны.

Рассмотрим теперь треугольники $(u+w)^*$, u_x, u_y и $(v+w)^*$, v_x, v_y. В силу следствия 1,

$$(u+w)^*+u_x=u_x+w_x=w_x+(u+w)^*,$$
$$(v+w)^*+v_x=v_x+w_x=w_x+(v+w)^*,$$

а из предположения (*) вытекает, что $(u+w)^*+u_x$ и $(v+w)^*+v_x$ являются различными прямыми. Следовательно,

$$[(u+w)^*+u_x]\cap[(v+w)^*+v_x]=w_x;$$

из тех же соображений видно, что

$$[(u+w)^*+u_y]\cap[(v+w)^*+v_y]=w_y.$$

Выше было показано, что прямые u_x+u_y и v_x+v_y различны; отсюда, принимая во внимание свойство (2.б), мы получаем, что

$$[u_x+u_y]\cap[v_x+v_y]=(x, y).$$

Точки w_x, w_y, (x, y) непременно коллинеарны; в силу утверждения (4), из совпадения между собой любых двух из этих точек следовало бы равенство $w_x = w_y$, которое противоречит нашему выбору индексов x и y. Таким образом, w_x, w_y и (x, y) являются тремя попарно различными коллинеарными точками. В силу выбора индексов x и y, прямые $u_x + v_x$ и $u_y + v_y$ различны. Из совпадения прямых $u_x + v_x$ и $(u+w)^* + (v+w)^*$ следовала бы доказываемая нами коллинеарность трех точек $(u+v)^*$, $(v+w)^*$, $(w+u)^*$, поскольку $(u+v)^* \leqslant u_x + v_x$; к такому же заключению о коллинеарности указанных точек мы пришли бы в случае совпадения прямых $u_y + v_y$ и $(u+w)^* + (v+w)^*$. Таким образом, нам, наконец, остается рассмотреть лишь случай, когда

$$u_x + v_x \neq (u+w)^* + (v+w)^* \neq u_y + v_y.$$

Но в этом случае можно воспользоваться теоремой, двойственной к теореме Дезарга (т. е. предложением 3 из § 3); в силу этой теоремы, три прямые $u_x + v_x$, $u_y + v_y$ и $(u+w)^* + (v+w)^*$ имеют общую точку. Но первые две прямые пересекаются в точке $(u+v)^*$ (по определению этой точки); этим коллинеарность трех точек $(u+v)^*$, $(v+w)^*$ и $(w+u)^*$ полностью доказана.

Следствие 2. *Если P и Q — различные точки и v, w — различные векторы, то:*

(а) *Существует самое большее один такой вектор u, что $(v+u)^* = P$ и $(w+u)^* = Q$.*

(б) *Тогда и только тогда существует такой вектор u, что $(v+u)^* = P$ и $(w+u)^* = Q$, когда P, Q и $(v+w)^*$ будут тремя попарно различными коллинеарными точками.*

Доказательство. Если существует такой вектор u, что

$$(v+u)^* = P \text{ и } (w+u)^* = Q,$$

то, поскольку $P \neq Q$, мы из предложения 4 выведем, что P, Q и $(v+w)^*$ являются тремя попарно различными коллинеарными точками. Предположим теперь, что P, Q и $(v+w)^* = R$ — три попарно различные коллинеарные точки. Поскольку ранг суммы координат вектора v не меньше 3, существует такой индекс x, что v_x является точкой, не лежащей на прямой $P+Q$. Допустим, что $w_x \leqslant P+Q$. Тогда, в силу следствия 1,

$$v_x + (v+w)^* = (v+w)^* + w_x \leqslant P+Q,$$

что невозможно, поскольку точка v_x не лежит на прямой $P+Q$. Следовательно, w_x является точкой, не лежащей на прямой $P+Q$. Отсюда вытекает, что $P+v_x$, $Q+w_x$ и $P+Q$ являются тремя попарно различными прямыми. Их суммой будет плоскость, поскольку, в силу следствия 1,

$$P + v_x + Q + w_x = P + (v+w)^* + v_x + w_x = P + (v+w)^* + v_x.$$

Поэтому $D=[P+v_x]\cap[Q+w_x]$ будет вполне определенной точкой, отличной от точек P и Q, поскольку точка P не лежит на прямой $Q+w_x$, а точка Q не лежит на прямой $P+v_x$.

Пусть теперь u' и u'' — такие векторы, что

$$P=(v+u')^*=(v+u'')^* \text{ и } Q=(w+u')^*=(w+u'')^*.$$

Тогда, в силу следствия 1,

$$u'_x+(v+u')^*=(v+u')^*+v_x=P+v_x,$$
$$u'_x+(w+u')^*=(w+u')^*+w_x=Q+w_x.$$

Отсюда вытекает, что координата u'_x отлична от 0 и содержится в D. Но тогда u'_x будет точкой, а так как и D является точкой, то нами показано, что $D=u'_x$. Подобным же образом можно убедиться в том, что $D=u''_x$. Следовательно, векторы u' и u'' удовлетворяют условиям $(v+u')^*=(v+u'')^*$ и $u'_x=u''_x$; отсюда и из предложения 3 вытекает, что $u'=u''$. Этим утверждение (а) полностью доказано.

Так как $v_x+P=P+D$, то, в силу предложения 3, существует такой (однозначно определенный) вектор u, что $(u+v)^*=P$ и $u_x=D$. Невозможно, чтобы было $u=w$, ибо тогда мы имели бы $(v+w)^*=(v+u)^*=P$. Теперь из предложения 4 и следствия 1 мы получаем, что

$$(u+w)^*\leqslant(u+v)^*+(v+w)^*=P+Q,$$
$$(u+w)^*\leqslant(u+w)^*+w_x=u_x+w_x=D+w_x=D+Q,$$

поскольку $(v+w)^*$, P, Q и Q, D, w_x составляют две тройки попарно различных коллинеарных точек[1]). Отсюда видно, что точка $(u+w)^*$ совпадает с точкой Q пересечения двух различных прямых $P+Q$ и $D+Q$. Таким образом, вектор u удовлетворяет всем нашим требованиям.

Замечание 2. В случае, когда $P=Q$, утверждение (а) перестает быть верным, а вместо утверждения (б) можно доказать следующее утверждение:

Тогда и только тогда существует такой вектор u, что $(v+u)^*=P=(w+u)^*$, когда $(v+w)^*=P$.

ПОСТРОЕНИЕ ОБЪЕМЛЮЩЕЙ ПРОЕКТИВНОЙ ГЕОМЕТРИИ

В частично упорядоченном множестве S, удовлетворяющем аксиомам I — IX, при условии, что ранг его максимального элемента A не меньше 3, мы выделили основной четырехугольник, состоящий из прямых L_x и точек (x, y). Опираясь на этот основ-

[1]) То, что точки D и w_x различны, следует из первого соотношения. — *Прим. перев.*

ной четырехугольник, мы определили векторы. Предыдущими рассмотрениями мы подготовлены к тому, чтобы построить объемлющую проективную геометрию $E(S)$. Элементами проективной геометрии $E(S)$ будут пары $X=[X_V, X_S]$, где X_V — (возможно, пустое) множество векторов, а X_S — элемент множества S; X_V и X_S связаны между собой следующими условиями:

(6.а) *Если v и w — векторы из X_V, то $(v+w)^* \leqslant X_S$.*

(6.б) *Если v и w — такие векторы, что $(v+w)^* \leqslant X_S$ и вектор v принадлежит X_V, то и вектор w принадлежит X_V.*

В системе $E(S)$ введем следующим образом частичное упорядочение:

(7) *$X' \leqslant X''$ тогда и только тогда, когда X'_V есть подмножество множества X''_V и $X'_S \leqslant X''_S$*[1]).

Через $H(S)$ мы обозначим подмножество всех тех элементов X системы $E(S)$, у которых компонентой X_V служит пустое множество. Очевидно, что отображая каждый элемент T из S на однозначно определенный элемент X из $H(S)$, имеющий компоненту $X_S=T$, мы получим проективное отображение частично упорядоченного множества S на частично упорядоченное множество $H(S)$.

Элементы из $E(S)$, не принадлежащие $H(S)$, следует изучить более детально.

Предложение 5. *Если X — элемент из $E(S)$ и если вектор v принадлежит X_V, то*

(а) *X_S является суммой всех элементов $(v+w)^*$, где w — вектор из X_V;*

(б) *X_V является совокупностью всех таких векторов w, что $(v+w)^*$ содержится в X_S.*

Доказательство. Обозначим через Y сумму всех элементов $(v+w)^*$, где w — вектор из X_V. Из условия (6.а) следует, что $Y \leqslant X_S$. Пусть P — произвольная точка, содержащаяся в X_S; тогда, в силу предложения 3 и замечания 1, существует такой вектор p, что $(v+p)^*=P$. Отсюда и из условия (6.б) вытекает, что p принадлежит X_V, и поэтому, по определению элемента Y, $P \leqslant Y$. Но согласно предложению 1 (§ 2), X_S является суммой всех содержащихся в X_S точек; следовательно, $Y=X_S$, и этим утверждение (а) доказано.

Обозначим теперь через Z совокупность таких векторов z, что $(v+z)^* \leqslant X_S$. По условию (6.а), X_V является частью совокупности Z, а из условия (6.б) следует, что X_V содержит Z; тем самым утверждение (б) доказано.

Следствие 3. *Если X' и X'' — такие элементы из $E(S)$, что их компоненты X'_V и X''_V равны и не пусты, то $X'=X''$.*

---

[1]) Легко проверить, что система $E(S)$ с так определенным соотношением порядка действительно удовлетворяет аксиомам I и II. — *Прим. перев.*

Это утверждение непосредственно следует из предложения 5 (а).

Предложение 6. *Если K — элемент из S, v — вектор и Θ — совокупность таких векторов w, что $(v+w)^* \leqslant K$, то $[\Theta, K]$ будет элементом системы $E(S)$.*

Доказательство. Пусть векторы w' и w'' принадлежат Θ. Тогда, в силу предложений 2 и 4,

$$(w'+w'')^* \leqslant (v+w')^* + (w''+v)^* \leqslant K,$$

и, следовательно, пара $[\Theta, K]$ удовлетворяет условию (6.а). Пусть теперь u', u'' — такие векторы, что $(u'+u'')^* \leqslant K$, причем вектор u' принадлежит Θ. Тогда, по определению совокупности Θ, $(v+u')^* \leqslant K$; отсюда и из тех же соображений, какими мы пользовались выше, вытекает, что

$$(v+u'')^* \leqslant (v+u')^* + (u'+u'')^* \leqslant K.$$

Таким образом, вектор u'' также принадлежит Θ, и этим показано, что пара $[\Theta, K]$ удовлетворяет условию (6.б). Следовательно, $[\Theta, K]$ является элементом системы $E(S)$.

Не боясь недоразумения, мы можем обозначить пустое множество векторов через 0. Тогда $[0, 0]$ будет *нулевым* (или минимальным) *элементом* частично упорядоченного множества $E(S)$. Если мы обозначим через $V(S)$ совокупность всех векторов, то $[V(S), A]$ будет *максимальным элементом* системы $E(S)$. Заметим, что максимальным элементом в подмножестве $H(S)$ является $[0, A]$.

Если v — произвольный вектор, то множество, состоящее из одного v, мы будем также обозначать через v; легко видеть, что $[v, 0]$ является элементом системы $E(S)$. Между элементами $[0, 0]$ и $[v, 0]$ нет, очевидно, промежуточных элементов, так что элементы вида $[v, 0]$ являются точками системы $E(S)$. Легко проверить, что все остальные точки из $E(S)$ имеют вид $[0, P]$, где P — точка множества S.

Предложение 7. *Система $E(S)$ удовлетворяет аксиомам* I — IX; *$[0, A]$ является гиперплоскостью системы $E(S)$.*

Доказательство. Система $E(S)$ является частично упорядоченным множеством, отношение порядка в котором определяется правилом (7); следовательно, $E(S)$ удовлетворяет аксиомам I и II. Прежде чем начать проверку справедливости остальных аксиом и свойств, введем следующее полезное *обозначение*. Если v — вектор и T — элемент из S, то через $T+v$ мы будем обозначать *совокупность таких векторов* w, что $(v+w)^* \leqslant T$. Из предложения 6 следует, что $[T+v, T]$ является элементом системы $E(S)$; используя предложение 5, легко убедиться, что каждый элемент из $E(S)$ имеет либо вид $[0, T]$, где T — элемент из S, либо вид $[T+v, T]$, где T — элемент из S и v — соответствующим образом выбранный вектор.

Рассмотрим теперь некоторое множество Φ элементов из $E(S)$. Множество всех элементов из Φ, имеющих вид $[0, T]$, обозначим через Φ', а совокупность остальных элементов из Φ обозначим через Φ''. Если элемент X_σ принадлежит Φ'', то множество $X_{\sigma V}$ не пусто и, следовательно, в нем можно некоторым способом выбрать вектор v_σ. Если совокупность Φ'' представляет собой пустое множество, то сумма всех элементов из Φ, очевидно, существует и имеет вид $[0, T]$, где T есть сумма всех элементов X из S, являющихся компонентами в элементах $[0, X]$ множества Φ (которое в этом случае совпадает с Φ'). Если же совокупность Φ'' содержит по крайней мере один элемент, то обозначим через v один из векторов v_σ. Образуем сумму $R = \sum\limits_{X \in \Phi} X_S + \sum\limits_{\sigma} (v + v_\sigma)^*$. Мы утверждаем, что $[R+v, R]$ является суммой всех элементов множества Φ. Действительно, из включения $(v+v_\sigma)^* \leqslant R$ следует, что $R+v$ содержит каждый вектор v_σ. Если X — элемент из Φ, то $X_S \leqslant R$ и $X = [0, X_S]$ или $X = [X_S + v_\sigma, X_S]$ для некоторого σ; следовательно, в обоих случаях $X \leqslant [R+v, R]$, и это включение справедливо для каждого X из Φ. Пусть теперь U — такой элемент системы $E(S)$, что $X \leqslant U$ для каждого X из Φ. Тогда $X_S \leqslant U_S$ для каждого X из Φ. Кроме того, v и все v_σ содержатся в U_V, и, следовательно, $(v+v_\sigma)^* \leqslant U_S$ для каждого σ. Таким образом, $R \leqslant U_S$; отсюда легко вытекает, что $R+v \leqslant U_V$. Этим показано, что $[R+v, R] \leqslant U$; тем самым мы убедились, что $[R+v, R]$ действительно является суммой всех элементов множества Φ.

Чтобы построить пересечение элементов множества Φ, обозначим через D пересечение всех компонент X_S элементов X из Φ. Если не существует вектора v, принадлежащего каждому множеству X_V, где $X \in \Phi$, то пересечением элементов множества Φ будет элемент $[0, D]$; если же вектор d, принадлежащий каждому X_V для X из Φ, существует, то пересечением элементов множества Φ будет элемент $[D+d, D]$. Этим показано, что в $E(S)$ выполняется аксиома III.

Нам полезно выписать явную формулу суммы двух элементов из $E(S)$. Возможны три случая:

$$[0, X] + [0, Y] = [0, X+Y];$$

$$[0, X] + [Y+v, Y] = [(X+Y)+v, X+Y];$$

$$[X+x, X] + [Y+y, Y] = [X+Y+(x+y)^*+x, X+Y+(x+y)^*],$$

где x, y, v — векторы, а X, Y — элементы множества S.

Прежде чем проверить справедливость в системе $E(S)$ закона Дедекинда, докажем следующее утверждение.

Лемма 1. *Если M, N — элементы множества S и m, n — векторы из $V(S)$, то следующие свойства эквивалентны:*

(I) *Существует вектор, принадлежащий одновременно* $M+m$ *и* $N+n$.

(II) $(m+n)^* \leqslant M+N$.

(III) $M \cap N < N \cap [M+(m+n)^*]$ *или* $(m+n)^* \leqslant M$.

Доказательство. Утверждение тривиально, если $m=n$, ибо в этом случае, в силу предложения 2, $(m+n)^*=0$. Поэтому мы будем предполагать, что $m \neq n$.

Пусть существует вектор v, принадлежащий одновременно $M+m$ и $N+n$. Тогда, по определению этих множеств векторов, $(m+v)^* \leqslant M$ и $(n+v)^* \leqslant N$; отсюда и из предложения 4 вытекает, что $(m+n)^* \leqslant (m+v)^* + (v+n)^* \leqslant M+N$. Таким образом, при выполнении свойства (I) выполняется и свойство (II).

Предположим теперь, что $(m+n)^* \leqslant M+N$ и $(m+n)^*$ не содержится в M. Тогда, используя закон Дедекинда, справедливый в множестве S, мы получаем, что

$$M < M+(m+n)^* = M+[(m+n)^* \cap (M+N)] =$$
$$= [M+N] \cap [(m+n)^* + M] = M+[N \cap (M+(m+n)^*)],$$

отсюда следует, что $M \cap N < N \cap [M+(m+n)^*]$. Тем самым показано, что при выполнении свойства (II) выполняется и свойство (III).

Пусть, наконец, справедливо свойство (III). Если $(m+n)^* \leqslant M$, то, по определению, вектор n принадлежит $M+m$ и, следовательно, является требуемым общим элементом множеств векторов $M+m$ и $N+n$. Подобным же образом m будет общим элементом указанных множеств векторов в случае, когда $(m+n)^* \leqslant N$. Поэтому предположим, что $(m+n)^*$ не содержится ни в M, ни в N. Тогда, в силу свойства (III),

$$M \cap N < N \cap [M+(m+n)^*];$$

отсюда и из предложения 1 (§ 2) следует существование точки P, содержащейся в $N \cap [M+(m+n)^*]$ и не содержащейся в $M \cap N$. Так как точка P принадлежит N, а точка $(m+n)^*$ к N не принадлежит, то $P \neq (m+n)^*$. Если бы $[P+(m+n)^*] \cap M$ было равно 0, то, используя закон Дедекинда, мы вывели бы, что

$$(m+n)^* = (m+n)^* + ([P+(m+n)^*] \cap M) =$$
$$= [P+(m+n)^*] \cap [M+(m+n)^*] =$$
$$= (m+n)^* + ([M+(m+n)^*] \cap P) = (m+n)^* + P,$$

откуда $P=(m+n)^*$, что невозможно. В то же время, так как точка $(m+n)^*$ не принадлежит M, то M не содержит прямую $P+(m+n)^*$; тем самым показано, что $Q=[P+(m+n)^*] \cap M$ является точкой. Принимая теперь во внимание, что точка Q принадлежит M, а точки P и $(m+n)^*$ к M не принадлежат, мы убеждаемся, что P, Q, $(m+n)^*$ являются тремя попарно различ-

ными коллинеарными точками. Но в таком случае, в силу следствия 2, существует, и притом только один, такой вектор h, что $(h+m)^* = Q$ и $(h+n)^* = P$. Так как $P \leqslant N$, то h принадлежит $N+n$; в то же время, поскольку $Q \leqslant M$, h принадлежит и $M+m$. Таким образом, h является общим вектором двух указанных множеств векторов; этим показано, что из свойства (III) следует свойство (I), чем завершается доказательство леммы.

Проверка в системе $E(S)$ закона Дедекинда. Пусть X, Y, Z — элементы из $E(S)$, и пусть $X \leqslant Y$. Тогда, очевидно,

$$X + (Y \cap Z) \leqslant Y \cap (X + Z). \qquad \text{(IV*)}$$

Рассмотрим теперь два случая.

Случай 1: по крайней мере одно из множеств X_V и Z_V пустое. В этом случае будет также пустым и хотя бы одно из множеств X_V и $(Y \cap Z)_V \leqslant Z_V$. Следовательно, по формуле сложения элементов из $E(S)$, мы получаем, что

$$X_S + Z_S = (X + Z)_S,$$

$$[X + (Y \cap Z)]_S = X_S + (Y \cap Z)_S = X_S + (Y_S \cap Z_S) =$$
$$= Y_S \cap (X_S + Z_S) = Y_S \cap (X + Z)_S = [Y \cap (X + Z)]_S.$$

Если множество $[Y \cap (X+Z)]_V$ пусто, то, в силу включения (IV*), множество $[X + (Y \cap Z)]_V$ будет также пустым, и, следовательно, в этом случае $X + (Y \cap Z) = Y \cap (X+Z)$. Предположим поэтому, что в $[Y \cap (X+Z)]_V$ существует вектор w. Этот вектор w принадлежит одновременно и Y_V и $(X+Z)_V$. Если w содержится в Z_V, то w содержится и в $(Y \cap Z)_V$ и, следовательно, множество $[X + (Y \cap Z)]_V$ будет непустым; то же самое справедливо и в случае, когда непустым является множество X_V. Рассмотрим теперь случай, когда множество X_V пусто и вектор w не принадлежит Z_V. Поскольку множество $(X+Z)_V$ не пусто, а множество X_V пусто, невозможно, чтобы было пустым Z_V. Следовательно, $Z_V = Z_S + z$ для некоторого вектора z. Далее, так как вектор w принадлежит $(X+Z)_V$, то $(X+Z)_V = (X+Z)_S + w = (X_S + Z_S) + w$. Принимая теперь во внимание, что вектор z содержится в Z_V, а поэтому и в $(X+Z)_V$, мы получаем, что

$$(z+w)^* \leqslant (X+Z)_S = X_S + Z_S.$$

Таким образом, выполняется условие (II) леммы 1; в силу же леммы 1, существует вектор v, принадлежащий одновременно $X_S + w$ и $Z_S + z$. В то же время, так как вектор w принадлежит к Y_V, то $X_S + w \leqslant Y_S + w = Y_V$; отсюда следует, что вектор v содержится в $Y_V \cap Z_V$, а потому и в $[X + (Y \cap Z)]_V$. Таким образом, в каждом из возможных случаев множество $[X + (Y \cap Z)]_V$ содержит некоторый вектор v, который, в силу включения (IV*), должен

содержаться и в $[Y \cap (X+Z)]_V$. Поэтому

$$X+(Y\cap Z) = [(X+(Y\cap Z))_S + v,\ (X+(Y\cap Z))_S] = \\ = [(Y\cap(X+Z))_S+v,\ (Y\cap(X+Z))_S] = Y\cap(X+Z),$$

и этим завершается проверка справедливости закона Дедекинда в случае 1.

Случай 2: ни одно из множеств X_V и Z_V не пусто. Обозначим через x и z векторы, содержащиеся соответственно в X_V и Z_V. Из формулы для суммы двух элементов из $E(S)$ вытекает, что

$$(X+Z)_S = X_S + Z_S + (x+z)^*;$$

используя теперь для элементов множества S закон Дедекинда, мы получаем

$$[Y\cap(X+Z)]_S = Y_S\cap[X_S+Z_S+(x+z)^*] = \\ = X_S+(Y_S\cap[Z_S+(x+z)^*]).$$

Последнее выражение в случае, когда

$$Y_S\cap Z_S = Y_S\cap[Z_S+(x+z)^*],$$

равно $X_S+(Y_S\cap Z_S)$; следовательно, в этом случае, используя включение (IV*), мы получаем, что

$$[Y\cap(X+Z)]_S = X_S+(Y_S\cap Z_S) \leqslant [X+(Y\cap Z)]_S \leqslant [Y\cap(X+Z)]_S,$$

откуда

$$[Y\cap(X+Z)]_S = [X+(Y\cap Z)]_S.$$

Если же

$$Y_S\cap Z_S < Y_S\cap[Z_S+(x+z)^*],$$

то, в силу леммы 1, существует вектор v, принадлежащий одновременно Y_S+x и Z_S+z. Но тогда, вектор v принадлежит и к $(Y\cap Z)_V = Y_V\cap Z_V$; поэтому, в силу формулы для суммы двух элементов из $E(S)$,

$$[X+(Y\cap Z)]_S = X_S+(Y\cap Z)_S+(x+v)^*.$$

Так как x принадлежит $X_V \leqslant Y_V$ и v принадлежит Y_V, то $(x+v)^* \leqslant Y_S$; аналогично, так как Z_V содержит оба вектора z и v, то $(z+v)^* \leqslant Z_S$. Из последнего включения и предложения 4 вытекает, что

$$(x+v)^* \leqslant (x+z)^* + (v+z)^* \leqslant (x+z)^* + Z_S.$$

Если бы элемент $(x+v)^*$ содержался в Z_S, то, в силу предложения 4, было бы

$$(x+z)^* \leqslant (x+v)^* + (v+z)^* \leqslant Z_S,$$

но это соотношение противоречит нашему предположению о том, что

$$Y_S\cap Z_S < Y_S\cap[Z_S+(x+z)^*].$$

Таким образом, принимая во внимание, что $(x+z)^*$ и $(x+v)^*$ являются точками, мы получаем, что

$$Z_S+(x+z)^*=Z_S+(x+v)^*.$$

Используя теперь включение $(x+v)^*\leqslant Y_S$ и закон Дедекинда, мы выводим, что

$$\begin{aligned}[Y\cap(X+Z)]_S&=X_S+(Y_S\cap[Z_S+(x+z)^*])=\\&=X_S+(Y_S\cap[Z_S+(x+v)^*])=\\&=X_S+(x+v)^*+(Y_S\cap Z_S)=[X+(Y\cap Z)]_S;\end{aligned}$$

таким образом, мы показали, что в случае 2 при любых обстоятельствах имеет место равенство $[Y\cap(X+Z)]_S=[X+(Y\cap Z)]_S$. Поскольку, кроме того, вектор x принадлежит $X_V\leqslant Y_V$, мы имеем

$$\begin{aligned}X+(Y\cap Z)&=[(X+(Y\cap Z))_S+x,\quad(X+(Y\cap Z))_S]=\\&=[(Y\cap(X+Z))_S+x,\quad(Y\cap(X+Z))_S]=Y\cap(X+Z),\end{aligned}$$

и этим полностью завершается наша проверка справедливости в системе $E(S)$ закона Дедекинда.

Проверка аксиомы V. (Принцип дополнения.) Напомним, что $[0,0]$ является нулевым элементом, а $[V, A]$, где V — множество всех векторов, — максимальным (или единичным) элементом системы $E(S)$. Пусть теперь X — произвольный элемент из $E(S)$. Согласно аксиоме V, справедливой в S, существует такой элемент C из S, что $0=X_S\cap C$, $A=X_S+C$. Если $X_V=0$, то положим $Y=[C+v, C]$, где v — произвольный (наугад выбранный) вектор; если же множество X_V не пусто, то положим $Y=[0, C]$. Таким образом, одно и только одно из множеств X_V и Y_V будет пустым, и, следовательно, $(X+Y)_S=X_S+C=A$. Так как одно из множеств X_V и Y_V содержит по крайней мере один вектор, который мы обозначим через w, то $(X+Y)_V$ также содержит вектор w. Поэтому $X+Y=[A+w, A]=[V, A]$. В то же время, так как одно из множеств X_V и Y_V пустое, то $X\cap Y=[0, X_S\cap C]=[0, 0]$. Таким образом, элемент Y является дополнением к X.

Проверка аксиомы VI. (Существование точек.) Если элемент X системы $E(S)$ отличен от нулевого элемента $[0,0]$, то либо X_V содержит вектор v, и в этом случае точка $[v, 0]$ будет частью X, либо $X_S\neq 0$, и тогда, в силу аксиомы VI, справедливой в S, X_S содержит точку P из S и, следовательно, X содержит точку $[0, P]$.

Проверка аксиомы VII. (Конечная зависимость.) Пусть Θ — некоторое множество элементов системы $E(S)$, и пусть Q — точка из $E(S)$, содержащаяся в сумме элементов множества Θ. Рассмотрим две возможности.

Случай 1: $Q=[0, P]$. Напомним, что компонента T_S суммы T элементов множества Θ представляет собой сумму всех ком-

понент X_S элементов X из Θ и всех точек вида $(v+w)^*$, где v и w — (различные) векторы из X_V для X из Θ. Так как P является точкой множества S, то из аксиомы VII, справедливой в S, и включения $P \leqslant T_S$ следует существование конечного числа таких элементов X_i из Θ и конечного числа таких векторов v_j, содержащихся в множествах X_V, где $X \in \Theta$, что

$$P \leqslant \sum_i (X_i)_S + \sum_{i \neq j} (v_i + v_j)^*.$$

Но отсюда уже видно, как нужно выбрать в Θ конечное число элементов Y_i, чтобы было $Q \leqslant \sum_i Y_i$.

Случай 2: $Q = [v, 0]$. Так как точка Q является частью суммы элементов множества Θ, то в Θ существует по крайней мере один элемент X, компонента которого X_V отлична от 0. Следовательно, в X_V существует вектор w. Если $v = w$, то $Q \leqslant X$. Если же $v \neq w$, то, в силу предложения 2, $(v+w)^*$ будет точкой. Так как обе точки $[v, 0]$ и $[w, 0]$ содержатся в сумме T элементов множества Θ, то в T содержится и сумма этих точек $[(v+w)^* + w, (v+w)^*]$; но в таком случае и точка $[0, (v+w)^*]$ является частью T. Воспользовавшись теперь результатом, полученным при рассмотрении случая 1, мы найдем в Θ конечное число таких элементов $X_1, \ldots, X_k$, что $[0, (v+w)^*] \leqslant \sum_{i=1}^{k} X_i$; но отсюда следует, что

$$Q \leqslant [(v+w)^* + w, (v+w)^*] = [w, 0] + [0, (v+w)^*] \leqslant X + \sum_{i=1}^{k} X_i,$$

и этим справедливость в системе $E(S)$ аксиомы VII полностью доказана.

Проверка аксиомы VIII. (Существование на прямой трех точек.) Предположим, что нам даны две различные точки M и N системы $E(S)$. Мы будем различать, естественно, три возможности.

Случай 1: $M = [m, 0]$ и $N = [n, 0]$. Так как точки M и N различные, то $m \neq n$ и, в силу предложения 2, $(m+n)^*$ будет точкой множества S. Отсюда и из формулы для суммы элементов из $E(S)$ вытекает, что $[0, (m+n)^*]$ является третьей точкой прямой $M + N = [(m+n)^* + m, (m+n)^*]$.

Случай 2: одна и только одна из точек M и N имеет вид $[0, P]$. Без ограничения общности можно предположить, что $M = [0, P]$, где P — точка из S. Тогда $N = [n, 0]$. В силу замечания 1, существует такой вектор v, что $(n+v)^* = P$. Из предложения 2 вытекает, что $n \neq v$; следовательно, $[v, 0]$ является третьей точкой прямой $M + N = [P + n, P]$.

Случай 3: $M=[0, P]$ и $N=[0, Q]$. В этом случае P и Q являются различными точками множества S; поэтому воспользуемся (справедливой в S) аксиомой VIII, в силу которой существует третья точка R прямой $P+Q$ из S. Но тогда $[0, R]$ будет третьей точкой прямой $M+N=[0, P+Q]$. Этим завершается проверка справедливости в системе $E(S)$ аксиомы VIII.

Доказательство утверждения, что $[0, A]$ является гиперплоскостью. Обозначим через v произвольный вектор из $V(S)$. Тогда максимальный элемент системы $E(S)$ можно представить в виде $[V, A]=[A+v, A]=[v, 0]\neq[0, A]$, где $[v, 0]$ является точкой системы $E(S)$. Поскольку $[0, A]\neq[V, A]$, из полученного равенства легко следует, что $[V, A]$ будет точкой над $[0, A]$, т. е. $[0, A]$ является гиперплоскостью системы $E(S)$.

Проверка аксиомы IX. (Теорема Дезарга.) Напомним, что ранг $r(A)$ не меньше 3 и что частично упорядоченное множество S (элементов, содержащихся в A) проективно эквивалентно частично упорядоченному множеству $H(S)$ элементов вида $[0, X]$, где $X\in S$. Поэтому $r([0, A])\geqslant 3$. Но $[0, A]$ является гиперплоскостью системы $E(S)$. Следовательно, $r([V, A])>3$. Отсюда и из предложения 2 (§ 3) вытекает, что в $E(S)$ справедлива теорема Дезарга. Этим предложение 7 полностью доказано.

§ 5. Группа гиперплоскости

Хотя наша цель состоит в том, чтобы результаты предыдущего параграфа применить к изучению гиперплоскости $[0, A]$, вложенной в частично упорядоченное множество $E(S)$, нам, однако, более удобно возвратиться в этом параграфе к тем обозначениям, которыми мы пользовались в первых трех параграфах настоящей главы. Итак, пусть S будет частично упорядоченным множеством, удовлетворяющим аксиомам I — IX. Максимальный элемент множества S обозначим через A; мы будем предполагать, что ранг элемента A не меньше трех. Обозначим, наконец, через H некоторую гиперплоскость множества S, которую мы будем считать фиксированной на протяжении всего нашего рассмотрения.

Группой $\Gamma=\Gamma(S, H)$ гиперплоскости H мы назовем совокупность всех перестановок σ частично упорядоченного множества S, обладающих следующими двумя свойствами:

(1.а) $M\leqslant N$ *тогда и только тогда, когда* $M\sigma\leqslant N\sigma$.

(1.б) $M\sigma=M$ *для каждого* $M\leqslant H$.

То, что совокупность перестановок σ множества S, обладающих свойствами (1.а) и (1.б), действительно является группой, вполне очевидно. На геометрическом языке такие перестановки σ мы могли бы называть перспективами с осью перспективы H.

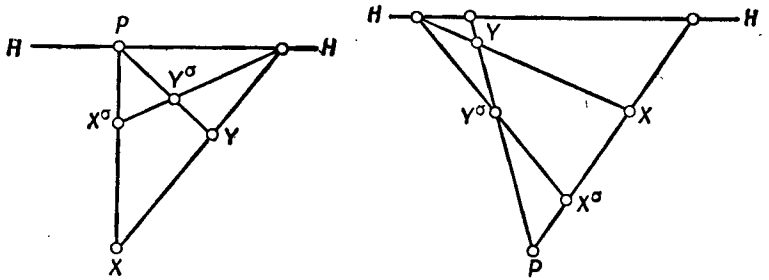
Если σ — перестановка из Γ и P — точка, обладающая свойством

(2) $M+P=M\sigma+P$ *для каждого элемента* M *из* S,

то точку P мы назовем *центром перестановки* σ (фиг. 19). Поскольку σ отображает точки на точки, ясно, что при перестановке σ центры этой перестановки остаются неподвижными.

Лемма 1. *Каждая отличная от* 1 *перестановка* σ *из* Γ *обладает одним и только одним центром, который мы обозначим через* $C(\sigma)$.

Доказательство. Пусть σ — перестановка из Γ, и пусть две различные точки P и Q являются центрами перестановки σ.



Фиг. 19.

Тогда, если точка X лежит на гиперплоскости H, то, в силу свойства (1.б), $X\sigma=X$. Если точка X не лежит ни на гиперплоскости H, ни на прямой $P+Q$, то, в силу свойства (2),

$$X+P=X\sigma+P \quad \text{и} \quad X+Q=X\sigma+Q.$$

Отсюда, принимая во внимание, что $X+P$ и $X+Q$ являются различными прямыми, мы получаем, что

$$X=[X+P]\cap[X+Q]=[X\sigma+P]\cap[X\sigma+Q]=X\sigma.$$

Если, наконец, точка X не лежит на гиперплоскости H, но лежит на прямой $P+Q$, то рассмотрим некоторую точку R, не лежащую ни на H, ни на $P+Q$ [существование такой точки R следует из того, что $r(A)\geqslant 3$]. Тогда, как было показано выше, $R\sigma=R$. Так как H есть гиперплоскость, а $R+X$ — прямая, не лежащая на H, то пересечением их $J=H\cap[R+X]$ будет точка, отличная от R и X; в силу свойства (1.б), $J\sigma=J$. Воспользовавшись теперь тем, что $R+X$ и $P+Q$ являются различными прямыми, мы получаем

$$X=(R+X)\cap(P+Q)=(R+J)\cap(P+Q)=$$
$$=(R\sigma+J\sigma)\cap(P\sigma+Q\sigma)=[(R+J)\cap(P+Q)]\,\sigma=X\sigma;$$

таким образом, мы показали, что при перестановке σ каждая точка множества S остается неподвижной. Но, в силу предложения 1 (§ 2), каждый элемент из S является суммой точек;

отсюда и из свойства (1.а) непосредственно следует, что $\sigma = 1$. Тем самым мы убедились, что каждая отличная от 1 перестановка из Γ обладает самое большее одним центром.

Пусть теперь σ — отличная от 1 перестановка из Γ. Рассмотрим два случая.

Случай 1: в S существует точка, неподвижная при перестановке σ и не лежащая на гиперплоскости H. Пусть J — такая точка, и пусть X — произвольная точка, не лежащая на H и отличная от J. Тогда прямая $J+X$ пересечет гиперплоскость H в некоторой точке Q, отличной от J и X. Очевидно, что $Q\sigma = Q$; следовательно,

$$X+J = J+Q = J\sigma + Q\sigma = (J+Q)\sigma = (J+X)\sigma = J\sigma + X\sigma = J + X\sigma;$$

отсюда легко вывести, что J является центром перестановки σ.

Случай 2: каждая точка, неподвижная при перестановке σ, принадлежит H. Рассмотрим сначала две различные точки X, Y, ни одна из которых не лежит на H. Тогда прямая $X+Y$ пересекает гиперплоскость H в точке J, которая остается неподвижной при перестановке σ. Кроме того, так как при перестановке σ ни одна из точек X и Y не остается неподвижной, то $X+X\sigma$ и $Y+Y\sigma$ будут вполне определенными прямыми. Далее,

$$X+X\sigma+Y+Y\sigma = X\sigma+X+J+Y\sigma = X\sigma+X+J\sigma+Y\sigma =$$
$$= X\sigma+X+(J+Y)\sigma = X\sigma+X+(X+Y)\sigma = X+X\sigma+Y\sigma.$$

Отсюда следует, что прямые $X+X\sigma$ и $Y+Y\sigma$ либо совпадают, либо по крайней мере компланарны. Если $X+X\sigma \neq Y+Y\sigma$, то эти прямые пересекаются по вполне определенной точке K. Прямая $X+X\sigma$ пересекает гиперплоскость H в некоторой точке K'; учитывая это, мы получаем

$$X+X\sigma = X\sigma+K' = X\sigma+K'\sigma = (X+K')\sigma = (X+X\sigma)\sigma.$$

Из тех же соображений видно, что $(Y+Y\sigma)\sigma = Y+Y\sigma$. Отсюда вытекает, что точка K пересечения прямых $X+X\sigma$ и $Y+Y\sigma$ при перестановке σ остается неподвижной, и, следовательно, она принадлежит H. Тем самым нами показано следующее:

Если X и Y — точки, не лежащие на гиперплоскости H, то прямые $X+X\sigma$ и $Y+Y\sigma$ при перестановке σ остаются инвариантными и $H \cap (X+X\sigma) = H \cap (Y+Y\sigma)$.

Отсюда следует, что все прямые $X+X\sigma$, где X — точки, не принадлежащие H, пересекаются с гиперплоскостью H в одной и той же точке, которая и будет центром перестановки σ. Этим лемма 1 полностью доказана.

Лемма 2. *Если P, Q, R — три попарно различные коллинеарные точки, причем ни точка P, ни точка Q не лежат на гиперплоскости H, то существует одна и только одна такая перестановка σ из Γ, что $C(\sigma) = R$ и $P\sigma = Q$.*

Доказательство. Предположим сначала, что существуют две перестановки σ' и σ'' из Γ, удовлетворяющие условиям $C(\sigma')=C(\sigma'')=R$ и $P\sigma'=P\sigma''=Q$. Тогда $\sigma'\sigma''^{-1}=\gamma$ будет такой перестановкой, принадлежащей Γ, что $P\gamma=P$ и $M+R=R+M\gamma$ для каждого элемента M из S. Так как $A=P+H$, то $P+M=(P+M)\cap(P+H)=P+[(P+M)\cap H]$, причем оба элемента P и $(P+M)\cap H$ при перестановке γ остаются неподвижными. Поэтому

$$P+M=P+[(P+M)\cap H]=P\gamma+[(P+M)\cap H]\gamma=$$
$$=(P+[(P+M)\cap H])\gamma=(P+M)\gamma=P\gamma+M\gamma=P+M\gamma,$$

и этим показано, что перестановка γ из Γ обладает двумя различными центрами P и R[1]). Отсюда и из леммы 1 вытекает, что $\gamma=1$ и, следовательно, $\sigma'=\sigma''$; таким образом, существует самое большее одна перестановка, удовлетворяющая нашим требованиям.

При доказательстве существования по крайней мере одной перестановки, удовлетворяющей нашим требованиям, нам удобно исключить из рассмотрения случай, когда одна (и, следовательно, каждая) прямая проходит точно через три различные точки. К случаю, когда каждая прямая проходит лишь через три точки, наш метод доказательства оказывается неприменимым; в этом случае, однако, можно использовать более простой, но вполне аналогичный метод. Детали, относящиеся к указанному случаю, мы оставляем в качестве упражнения читателю.

Рассмотрим произвольную прямую L, проходящую через точку P и отличную от прямой $P+R$. Так как прямая L проходит через одну и только одну точку $L\cap H$ гиперплоскости H, то на L можно найти такие две точки P', P'', не лежащие на H, что P, P', P'' будут тремя попарно различными точками прямой L. Тогда $P+R$, $P'+R$ и $P''+R$ будут тремя попарно различными прямыми, проходящими через точку R и лежащими в плоскости $L+R$; отметим, что ни одна из этих трех прямых не лежит в гиперплоскости H. Отсюда, как обычно, следует, что

$$Q'=[(L\cap H)+Q]\cap[P'+R],\quad Q''=[(L\cap H)+Q]\cap[P''+R]$$

представляют собой вполне определенные точки, не принадлежащие гиперплоскости H. Заметим, что четыре точки Q, Q', Q'', $L\cap H$ попарно различны и коллинеарны.

Рассмотрим теперь точку X, отличную от R и не принадлежащую H. В таком случае точка X может лежать самое большее на одной из трех прямых $P+R$, $P'+R$ и $P''+R$. Предположим, что точка X не лежит на прямых $P+R$ и $P'+R$, и рассмотрим два случая.

[1]) То, что P является центром перестановки γ, непосредственно следует из доказательства леммы 1 (случай 1).—*Прим. перев.*

Случай 1: точки X, P, P' коллинеарны. В этом случае прямая $L=X+P=P+P'=P'+X$ пересекает гиперплоскость H в точке $L\cap H$, а прямая $Z=(H\cap L)+Q=(H\cap L)+Q'$ пересекает прямую $X+R$ по вполне определенной точке $(X+R)\cap Z$.

Случай 2: точки X, P, P' не коллинеарны. В этом случае прямая $X+P$ пересекает гиперплоскость H в точке $H\cap(X+P)$, а прямая $X+P'$ пересекает H в некоторой другой точке $H\cap(X+P')$. Треугольники P, Q, $(P+X)\cap H$ и P', Q', $(P'+X)\cap H$ перспективны с центром перспективы в точке $(P+P')\cap H=(Q+Q')\cap H=L\cap H$, поскольку плоскость $L+X$ пересекает гиперплоскость H по прямой, проходящей через точки $L\cap H$, $(P+X)\cap H$, $(P'+X)\cap H$; соответствующие стороны этих треугольников пересекаются в точках

$$(P+Q)\cap(P'+Q')=R,$$

$$(P+[(P+X)\cap H])\cap(P'+[(P'+X)\cap H])=(P+X)\cap(P'+X)=X,$$

$$(Q+[(P+X)\cap H])\cap(Q'+[(P'+X)\cap H]).$$

Используя теперь теорему Дезарга (аксиому IX), мы получаем, что прямые $X+R$, $Q+[(P+X)\cap H]$ и $Q'+[(P'+X)\cap H]$ пересекаются в одной точке, так что

$$(X+R)\cap(Q+[(P+X)\cap H])=(X+R)\cap(Q'+[(P'+X)\cap H]).$$

Результат, полученный при рассмотрении случаев 1 и 2, мы сформулируем следующим образом:

(*) Если точка X не лежит ни на одной из прямых $P+R$ и $P'+R$ (и не лежит на гиперплоскости H), то

$$(X+R)\cap(Q+[(P+X)\cap H])=(X+R)\cap(Q'+[(P'+X)\cap H])$$

является вполне определенной точкой.

Аналогичные утверждения справедливы для случаев, когда точка X не лежит ни на одной из прямых $P'+R$ и $P''+R$, и т. д.

Теперь мы подготовлены к тому, чтобы определить следующим образом отображение точек X на точки X^*:

$X^*=X$, если $X=R$ или если $X\leqslant H$;

$X^*=(X+R)\cap(Q+[(P+X)\cap H])$, если X не лежит на $P+R$;

$X^*=(X+R)\cap(Q'+[(P'+X)\cap H])$, если X не лежит на $P'+R$;

$X^*=(X+R)\cap(Q''+[(P''+X)\cap H])$, если X не лежит на $P''+R$.

Из леммы (*) следует, что так определенное отображение * является однозначным отображением точек в точки. Переставляя между собой символы P и Q, мы получаем другое однозначное отображение $^+$ точек в точки; используя закон Дедекинда, нетрудно проверить, что эти два отображения являются взаимно обратными.

Следовательно, отображение * в действительности является перестановкой точек множества S, оставляющей неподвижными только точку R и точки гиперплоскости H.

Пусть теперь X и Y—две различные точки, каждая из которых отлична от R и не принадлежит H. В таком случае невозможно, чтобы на каждой из трех прямых $P+R$, $P'+R$, $P''+R$ лежала по крайней мере одна из точек X и Y; поэтому без ограничения общности мы можем предположить, что ни точка X, ни точка Y не лежат на прямой $P+R$. Если прямые $X+Y$ и X^*+Y^* окажутся равными, то они, естественно, пересекают гиперплоскость H в одной и той же точке. Предположим теперь, что $X+Y$ и X^*+Y^*— различные прямые. Отсюда, в частности, следует, что различными будут прямые $X+X^*$ и $Y+Y^*$. Рассмотрим треугольники P, X, Y и Q, X^*, Y^*. Они перспективны с центром перспективы в точке R (в силу определения отображения * и выбора точек P и Q), и три прямые, проходящие через перспективные вершины этих треугольников, различны. Соответствующие стороны рассматриваемых треугольников пересекаются в точках

$$(P+X)\cap(Q+X^*)=(P+X)\cap H,$$
$$(P+Y)\cap(Q+Y^*)=(P+Y)\cap H,$$
$$(X+Y)\cap(X^*+Y^*).$$

Применяя теперь теорему Дезарга (аксиому IX), мы получаем, что точки

$$(P+X)\cap H,\ (P+Y)\cap H,\ (X+Y)\cap(X^*+Y^*)$$

коллинеарны. Поскольку первые две из этих точек принадлежат H, то же самое справедливо и относительно третьей точки. Отсюда, принимая во внимание, что прямые $X+Y$ и X^*+Y^* не лежат в гиперплоскости H, мы выводим, что указанные прямые пересекаются с H в одной и той же точке. Теперь легко убедиться в справедливости следующего утверждения.

(**) Если X и Y—две различные точки, каждая из которых не принадлежит гиперплоскости H, то

$$(X+Y)\cap H=(X^*+Y^*)\cap H.$$

Отметим, наконец, тот очевидный факт, что $P^*=Q$.

Пусть теперь M—произвольный элемент множества S. Тогда мы определим $M\sigma$ как сумму всех точек X^*, где X—точки, содержащиеся в M.

Очевидно, что $0\sigma=0$, $A\sigma=A$ и $X\sigma=X^*$ для каждой точки X. Далее, пусть точка $Y\leqslant M\sigma$. Существует, и притом только одна, такая точка X, что $X^*=Y$. Мы хотим показать, что $X\leqslant M$. Действительно, из определения элемента $M\sigma$ и аксиомы VII

непосредственно следует существование конечного (минимального) числа таких точек $X_1, \ldots, X_k$, содержащихся в M, что $X^* \leqslant \sum_{i=1}^{k} X_i^*$. Если $k=1$, то $X^* = X_1^*$; отсюда и из взаимной однозначности отображения * вытекает, что $X = X_1$. Поэтому мы можем по индукции предположить, что точка Z содержится в $\sum_{i=1}^{k-1} X_i$ всякий раз, когда $Z^* \leqslant \sum_{i=1}^{k-1} X_i^*$, причем $k > 1$. Так как k есть минимальное число точек $X_1, \ldots, X_k$, удовлетворяющих условию $X^* \leqslant \sum_{i=1}^{k} X_i^*$, то $X^* \neq X_k^*$. Следовательно, $X^* + X_k^*$ является прямой; используя закон Дедекинда, мы выводим, что

$$X^* + X_k^* = [X^* + X_k^*] \cap [\sum_{i=1}^{k} X_i^*] = X_k^* + [(X^* + X_k^*) \cap \sum_{i=1}^{k-1} X_i^*].$$

Поскольку $X^* + X_k^*$ является прямой, а X_k^*—точкой, и так как точка X^* не содержится в $\sum_{i=1}^{k-1} X_i^*$ (в силу минимальности числа k), то из предыдущего равенства следует, что

$$Z^* = (X^* + X_k^*) \cap \sum_{i=1}^{k-1} X_i^*$$

будет точкой. Но $Z^* \leqslant \sum_{i=1}^{k-1} X_i^*$; отсюда и из нашего индуктивного предположения вытекает, что точка Z содержится в $\sum_{i=1}^{k-1} X_i$. Если бы Z^* совпадала с X_k^*, то точка X_k^* содержалась бы в $\sum_{i=1}^{k-1} X_i^*$, но это противоречит минимальности числа k; из тех же соображений видно, что $Z^* \neq X^*$. Следовательно, $L^* = X^* + Z^* = Z^* + X_k^* = X_k^* + X^*$ является прямой. Если одна из трех точек X, Z, X_k принадлежит гиперплоскости H, то коллинеарность трех точек X, Z, X_k следует из утверждения (**) и коллинеарности точек X^*, Z^*, X_k^*. Если же ни одна из трех точек X, Z, X_k не лежит на H, то $L^* \cap H$ будет точкой, отличной от X, Z, X_k (здесь нужно принять во внимание, что H является гиперплоскостью и что каждая точка, содержащаяся в H, при отображении * остается неподвижной). В то же время из утверждения (**) вытекает, что точка $L^* \cap H$ принадлежит всем трем прямым $X + Z$, $Z + X_k$ и $X_k + X$; отсюда следует, что и в этом случае точки

X, Z, X_k коллинеарны. Поэтому

$$X \leqslant Z + X_k \leqslant \sum_{i=1}^{k-1} X_i + X_k \leqslant M.$$

Таким образом, методом индукции мы показали, что точка X тогда и только тогда содержится в M, когда точка X^* содержится в $M\sigma$. Отсюда и из предложения 1 (§ 2) легко следует, что σ является перестановкой элементов множества S, обладающей свойством (1.a). Так как $X^* = X$ для каждой точки X гиперплоскости H, то и $M\sigma = M$ для каждого элемента $M \leqslant H$. Наконец, $P\sigma = P^* = Q$ и $X + R = X^* + R = X\sigma + R$ для каждой точки X. Из последнего соотношения непосредственно следует, что точка R является центром перестановки σ; этим лемма 2 полностью доказана.

Лемма 3. *Если каждая из перестановок* σ', σ'' *и* $\sigma'\sigma''$, *принадлежащих группе* Γ, *отлична от* 1, *то* $C(\sigma'\sigma'') \leqslant C(\sigma') + C(\sigma'')$.

Доказательство. Если $C(\sigma') = C(\sigma'') = Z$, то, в силу свойства (2),

$$M + Z = M\sigma' + Z = (M\sigma')\sigma'' + Z = M(\sigma'\sigma'') + Z;$$

отсюда и из леммы 1 следует, что $C(\sigma'\sigma'') = Z = C(\sigma') = C(\sigma'')$. Предположим теперь, что $C(\sigma')$ и $C(\sigma'')$—различные точки. Выберем прямую L, не лежащую в гиперплоскости H и не проходящую ни через одну из точек $C(\sigma')$, $C(\sigma'')\sigma'^{-1}$ и $C(\sigma'\sigma'')$[1]. Прямая L проходит через точку $L \cap H$ гиперплоскости H и еще по крайней мере через две различные точки X и Y, не содержащиеся в H. Так как

$$L \cap H = (L \cap H)\sigma' = (L \cap H)\sigma'' = (L \cap H)\sigma'\sigma'',$$

то через точку $L \cap H$ проходят все три прямые

$$L = X + Y, \quad L\sigma' = X\sigma' + Y\sigma' \quad \text{и} \quad L\sigma'\sigma'' = X\sigma'\sigma'' + Y\sigma'\sigma''.$$

Отсюда следует, что треугольники X, $X\sigma'$, $X\sigma'\sigma''$ и Y, $Y\sigma'$, $Y\sigma'\sigma''$ перспективны с центром перспективы в точке $L \cap H$; прямые $X + Y = L$, $L\sigma'$ и $L\sigma'\sigma''$ различные, так как в противном случае либо хотя бы одна из точек $C(\sigma')$ и $C(\sigma'\sigma'')$ лежала бы на прямой L, либо точка $C(\sigma'')$ лежала бы на прямой $L\sigma'$. Легко проверить, что прямые $X + X\sigma'$ и $Y + Y\sigma'$ различны и пересекаются в точке $C(\sigma')$, что прямые $X\sigma' + X\sigma'\sigma''$ и $Y\sigma' + Y\sigma'\sigma''$ пересекаются в точке $C(\sigma'')$ и что прямые $X + X\sigma'\sigma''$ и $Y + Y\sigma'\sigma''$ пересекаются в точке $C(\sigma'\sigma'')$. Применяя теперь теорему Дезарга, мы получаем,

[1]) Здесь автор, очевидно, предполагает, что каждая прямая проходит более чем через три точки. В случае, когда на каждой прямой лежат лишь три точки, лемму можно доказать методом от противного.—*Прим. перев.*

что точки $C(\sigma')$, $C(\sigma'')$ и $C(\sigma'\sigma'')$ коллинеарны, чем завершается доказательство леммы 3.

Если σ—перестановка из Γ, то либо $\sigma = 1$, и в этом случае каждая точка множества S будет центром перестановки σ, либо $\sigma \neq 1$, и тогда, в силу леммы 1, σ обладает одним и только одним центром $C(\sigma)$. Если M—отличный от 0 элемент множества S, то, как следует из леммы 3, *совокупность* $\Gamma(M)$ *перестановок* σ *из* Γ, *центры которых* $C(\sigma)$ *содержатся в* M, *является подгруппой группы* Γ.

Положим $\Gamma(0) = 1$. Очевидно, что $\Gamma = \Gamma(A)$. Нас особенно будет интересовать подгруппа $\Gamma(H) = B$.

Теорема 1 (а). *B является нормальным делителем группы Γ.*

(б) *Группа B коммутативна (абелева).*

(в) *Отображение каждого элемента M из S, содержащегося в H, на подгруппу $\Gamma(M) \leqslant B$ является проективным.*

(г) *Эндоморфизмы η группы B, удовлетворяющие условию $\Gamma(M)^\eta \leqslant \Gamma(M)$ для каждого элемента $M \leqslant H$, образуют тело F.*

(д) *Подгруппа T группы B тогда и только тогда удовлетворяет условию $T^F \leqslant T$ [1]), когда $T = \Gamma(N)$ для некоторого элемента $N \leqslant H$.*

Доказательство. Если σ' и σ''—перестановки из Γ и $\sigma' \neq 1$, то, в силу свойства (2),

$$M + C(\sigma')\sigma'' = [M\sigma''^{-1} + C(\sigma')]\,\sigma'' =$$

$$= [M\sigma''^{-1}\sigma' + C(\sigma')]\,\sigma'' = M\sigma''^{-1}\sigma'\sigma'' + C(\sigma')\sigma'';$$

отсюда следует, что $C(\sigma''^{-1}\sigma'\sigma'') = C(\sigma')\sigma''$. Если, в частности, $C(\sigma') \leqslant H$, то $C(\sigma''^{-1}\sigma'\sigma'') = C(\sigma')\sigma'' = C(\sigma')$; следовательно, $\sigma^{-1}B\sigma = B$ для каждого σ из Γ, и этим утверждение (а) доказано.

Пусть теперь σ', σ''—такие отличные от 1 элементы группы B, что $C(\sigma') \neq C(\sigma'')$. В таком случае $C(\sigma')$ и $C(\sigma'')$ будут двумя различными точками гиперплоскости H. Рассмотрим произвольную точку P, не принадлежащую H. Тогда точки P, $P\sigma'$, $C(\sigma')$, так же, как и точки P, $P\sigma''$, $C(\sigma'')$, будут коллинеарными. Так как прямые $L' = P + P\sigma'$ и $L'' = P + P\sigma''$ пересекают гиперплоскость H соответственно в точках $C(\sigma')$ и $C(\sigma'')$, то прямые L' и L'' различны и пересекаются в точке P. (Заметим, что неравенства $P \neq P\sigma'$ и $P \neq P\sigma''$ нетрудно вывести из леммы 1 и ее доказательства.) Теперь легко проверить, что

$$P\sigma'\sigma'' = [P\sigma' + C(\sigma'')] \cap [P\sigma'' + C(\sigma')] = P\sigma''\sigma',$$

но отсюда и из леммы 1 легко вывести, что $\sigma'\sigma'' = \sigma''\sigma'$.

---

[1]) Через T^F обозначается множество перестановок вида σ^η, где σ—перестановка из T и η—эндоморфизм из F.—*Прим. перев.*

Если же σ' и σ''—перестановки из B с одним и тем же центром $C(\sigma')=C(\sigma'')$, то, в силу леммы 2, можно построить такую перестановку $\sigma \neq 1$, принадлежащую B, что $C(\sigma) \neq C(\sigma')=C(\sigma'')$. Из свойства (2) легко следует, что $C(\sigma^{-1})=C(\sigma)$; используя это замечание и результат предыдущего абзаца, мы получаем, что $\sigma\sigma'=\sigma'\sigma$ и $\sigma^{-1}\sigma''=\sigma''\sigma^{-1}$. Если бы центр $C(\sigma'\sigma)$ совпадал с центром $C(\sigma^{-1}\sigma'')$, то, согласно лемме 3, оба эти центра совпали бы с центрами $C(\sigma'\sigma\sigma^{-1}\sigma'')=C(\sigma'\sigma'')=C(\sigma')=C(\sigma'')$. Но тогда из равенства $C(\sigma'\sigma)=C(\sigma')$ следовало бы равенство $C(\sigma')=C(\sigma'^{-1}\sigma'\sigma)=$ $=C(\sigma)$, которое противоречит выбору перестановки σ. Таким образом, $C(\sigma'\sigma) \neq C(\sigma^{-1}\sigma'')$; отсюда и из результата предыдущего абзаца вытекает, что

$$\sigma'\sigma''=\sigma'\sigma\sigma^{-1}\sigma''=\sigma^{-1}\sigma''\sigma'\sigma=\sigma''\sigma^{-1}\sigma\sigma'=\sigma''\sigma';$$

тем самым коммутативность группы B доказана [заметим, что в процессе этого доказательства мы пользовались тем, что $r(H)>1$].

Пусть теперь T' и T''—такие элементы из S, что $T'<T''\leqslant H$. Тогда, как непосредственно следует из определения групп $\Gamma(T)$, $\Gamma(T')\leqslant\Gamma(T'')\leqslant\Gamma(H)=B$. Так как $T'<T''$, то, в силу предложения 1 (§ 2), существует точка P, лежащая на T'' и не лежащая на T'. По лемме 2, в Γ существует такая перестановка $\sigma \neq 1$, что $C(\sigma)=P$. Перестановка σ содержится, очевидно, в $\Gamma(T'')$ и не содержится в $\Gamma(T')$; этим показано, что $\Gamma(T')<\Gamma(T'')$. Отсюда непосредственно следует справедливость нашего утверждения (в).

Обозначим через F совокупность всех эндоморфизмов η группы B, удовлетворяющих условию

$$\Gamma(M)^{\eta}\leqslant\Gamma(M) \text{ для каждого элемента } M\leqslant H.$$

Поскольку группа B коммутативна, сумма, разность и произведение эндоморфизмов группы B также будут эндоморфизмами этой группы (см. гл. V, § 1); принимая это во внимание, легко убедиться в том, что F является кольцом.

Рассмотрим теперь произвольный элемент η кольца F. Пусть σ' и σ''—такие отличные от 1 элементы группы B, что $C(\sigma') \neq C(\sigma'')$. Тогда $C(\sigma'\sigma'')$ будет точкой прямой $C(\sigma')+C(\sigma'')$, отличной от каждой из точек $C(\sigma')$ и $C(\sigma'')$. Предположим, что $\sigma'^{\eta}=1$. Тогда $(\sigma'\sigma'')^{\eta}=\sigma''^{\eta}$, но $(\sigma'\sigma'')^{\eta}$ принадлежит $\Gamma[C(\sigma'\sigma'')]$, а σ''^{η} принадлежит $\Gamma[C(\sigma'')]$. Поскольку же точки $C(\sigma'')$ и $C(\sigma'\sigma'')$ различны, мы имеем $\Gamma[C(\sigma'\sigma'')]\cap\Gamma[C(\sigma'')]=1$, и, следовательно, $\sigma''^{\eta}=1$. Предположим теперь, что $\eta \neq 0$. В таком случае в B существует такая перестановка σ, что $\sigma^{\eta} \neq 1$. Поэтому, если центр $C(\sigma')$ перестановки σ' не совпадает с $C(\sigma)$, то, как мы только что показали, и $\sigma'^{\eta} \neq 1$. Если же $\sigma' \neq 1$, но $C(\sigma')=C(\sigma)$, то, в силу

леммы 2, существует такая перестановка σ'', принадлежащая B, что

$$C(\sigma'') \neq C(\sigma) = C(\sigma').$$

В таком случае, как было показано выше, $\sigma''^{\eta} \neq 1$, а отсюда следует, что и $\sigma'^{\eta} \neq 1$. Таким образом, мы убедились, что

(г.1) *если η—ненулевой эндоморфизм из F, то η определяет взаимно однозначное отображение группы B в себя.*

Если σ—произвольный элемент группы Γ, то, поскольку, как было показано выше, B является нормальным делителем группы Γ, мы получим автоморфизм группы B, отображая каждый элемент β из B на элемент $\beta^{\sigma} = \sigma^{-1}\beta\sigma$. Принимая во внимание, что $C(\beta) \leqslant H$ для каждого β из B, и используя замечание, сделанное в начале доказательства, мы получаем, что $C(\beta) = C(\sigma^{-1}\beta\sigma) = C(\beta^{\sigma})$. Отсюда легко следует, что $\Gamma(M)^{\sigma} = \Gamma(M)$ для каждого $M \leqslant H$; тем самым показано, что автоморфизм, индуцированный в группе B внутренним автоморфизмом группы Γ, принадлежит кольцу F. Покажем теперь, что (за исключением одного тривиального случая) справедливо и обратное утверждение, а именно:

(г. 2) *Если η — отличный от 0 элемент кольца F, то существует такой элемент σ группы Γ, что $\beta^{\eta} = \beta^{\sigma}$ для каждого β из B.*

Наше утверждение, очевидно, справедливо, если η является тождественной перестановкой. Поэтому без ограничения общности можно предположить, что в B существует такой элемент τ, для которого $\tau^{\eta} \neq \tau$. Из утверждения (г. 1) вытекает, что ни τ, ни τ^{η} не являются тождественными перестановками. Так как η принадлежит F, то $C(\tau) = C(\tau^{\eta})$. В то же время $\tau \neq \tau^{\eta}$ и, следовательно, существует такая точка P, что $P\tau \neq P\tau^{\eta}$. Поскольку τ и τ^{η} принадлежат B, они оставляют неподвижными те и только те точки, которые лежат на гиперплоскости H. Отсюда вытекает, что точка P не принадлежит H и что P, $P\tau$, $P\tau^{\eta}$ являются тремя попарно различными точками. Согласно свойству (2), точки P, $P\tau$, $C(\tau)$, так же, как и точки P, $P\tau^{\eta}$, $C(\tau^{\eta}) = C(\tau) = Z$, коллинеарны. Следовательно, P, $P\tau$, $P\tau^{\eta}$, Z представляют собой четверку попарно различных коллинеарных точек. Отсюда и из леммы 2 вытекает существование в группе Γ одной и только одной перестановки σ, такой, что $P = C(\sigma)$ и $P\tau^{\eta} = P\tau\sigma$. Так как точка P остается неподвижной при перестановке σ, то эта точка остается неподвижной и при перестановке σ^{-1}; но отсюда следует, что

$$P\tau\sigma = P\sigma^{-1}\tau\sigma = P\tau^{\sigma} = P\tau^{\eta}.$$

Заметим, что τ^{σ} принадлежит B и $C(\tau^{\sigma}) = C(\tau)$. Таким образом, τ^{η} и τ^{σ} являются перестановками из B, имеющими один и тот

же центр Z; они одинаково действуют на точку P, отличную от центра этих перестановок и не лежащую на гиперплоскости H. Отсюда и из леммы 2 вытекает, что $\tau^\sigma = \tau^\eta$. Рассмотрим теперь эндоморфизм χ, принадлежащий F и определяемый равенством $\beta^\chi = \beta^{\eta - \sigma}$ для каждого β из B (так что эндоморфизм χ отличается от эндоморфизма η на автоморфизм, индуцированный элементом σ из Γ). Эндоморфизм χ отображает элемент $\tau \neq 1$ на $\tau^\chi = \tau^{\eta - \sigma} = 1$. Следовательно, в силу утверждения (г. 1), $\chi = 0$; но это означает, что $\beta^\eta = \beta^\sigma$ для каждого β из B. Таким образом, утверждение (г. 2) полностью доказано.

Из утверждения (г. 2) непосредственно вытекает, что каждый отличный от 0 элемент η кольца F представляет собой автоморфизм группы B, обладающий, естественно, обратным автоморфизмом, который также принадлежит F. Следовательно, F является телом, и этим утверждение (г) полностью доказано.

Из определения тела F вытекает, что $\Gamma(M)^F \leqslant \Gamma(M)$ для каждого элемента $M \leqslant H$ (в действительности здесь имеет место равенство, ибо тело F содержит единицу). Обратно, пусть T — подгруппа группы B, удовлетворяющая условию $T^F \leqslant T$. Тогда мы прежде всего покажем, что

(д. 1) *если σ — отличный от 1 элемент подгруппы T и если σ' — такая перестановка из B, что $C(\sigma) = C(\sigma')$, то σ' принадлежит T.*

Действительно, положим $Z = C(\sigma) = C(\sigma')$. Тогда Z является точкой гиперплоскости H, ибо σ принадлежит $T \leqslant B$. Так как σ и σ' — отличные от 1 перестановки из B, то они оставляют неподвижными лишь точки гиперплоскости H (и каждая точка, лежащая на H, остается неподвижной при этих перестановках). Пусть теперь P — произвольная точка, не лежащая на H. Тогда $P\sigma \neq P$ и $P\sigma' \neq P$, причем точки P, $P\sigma$, $P\sigma'$, Z коллинеарны. Если $P\sigma = P\sigma'$, то, по лемме 2, $\sigma = \sigma'$; предположим поэтому, что $P\sigma \neq P\sigma'$. Тогда, в силу леммы 2, в Γ существует такая перестановка σ'', что $P = C(\sigma'')$ и $P\sigma = P\sigma'\sigma''$. Проведя точно такие же рассуждения, какими мы пользовались выше (при доказательстве утверждения (г. 2)), мы покажем, что $\sigma = \sigma''^{-1}\sigma'\sigma''$, откуда $\sigma' = \sigma''\sigma\sigma''^{-1} = \sigma^{\sigma''-1}$. Но σ'' и σ''^{-1} индуцируют автоморфизмы группы B, принадлежащие F; следовательно, σ' принадлежит $\sigma^F \leqslant T^F \leqslant T$, что и требовалось доказать.

(д. 2) *Если σ' и σ'' — отличные от 1 перестановки из T и если $C(\sigma) \leqslant C(\sigma') + C(\sigma'')$, то σ принадлежит T.*

В случае, когда $C(\sigma') = C(\sigma'')$, наше утверждение непосредственно следует из утверждения (д. 1). Предположим поэтому, что $C(\sigma') \neq C(\sigma'')$; заметим, что прямая $C(\sigma') + C(\sigma'')$ лежит в гиперплоскости H. Наше утверждение также следует из утверждения (д. 1) в случае, когда $C(\sigma)$ совпадает либо с $C(\sigma')$, либо с $C(\sigma'')$; таким образом, мы можем теперь предположить, что $C(\sigma)$, $C(\sigma')$

и $C(\sigma'')$ являются тремя попарно различными коллинеарными точками. Рассмотрим произвольную точку P, не лежащую на H. В таком случае P, $P\sigma'$, $C(\sigma')$ будут тремя попарно различными коллинеарными точками; прямые

$$P + C(\sigma) \text{ и } P\sigma' + C(\sigma'')$$

— двумя различными прямыми, лежащими в плоскости $P + C(\sigma') + C(\sigma'')$. Следовательно, эти прямые пересекаются во вполне определенной точке $Q = [P + C(\sigma)] \cap [P\sigma' + C(\sigma'')]$, не лежащей на гиперплоскости H. В силу леммы 2, в Γ существует, и притом только одна, такая перестановка τ, что $C(\tau) = C(\sigma'')$ и $P\sigma'\tau = Q$. Очевидно, что τ принадлежит B; поскольку σ'' содержится в T, из утверждения (д. 1) вытекает, что и τ содержится в T. Но в таком случае в T содержится и $\sigma'\tau$, ибо σ' и τ являются элементами подгруппы T группы B. Принимая теперь во внимание, что $P\sigma'\tau = Q$, мы получаем равенство $C(\sigma'\tau) = H \cap [P + Q] = C(\sigma)$, из которого, в силу утверждения (д. 1), вытекает, что само σ принадлежит T; тем самым утверждение (д. 2) доказано.

(д. 3) *Если* $\sigma_1, \ldots, \sigma_n$ *— конечное число отличных от* 1 *перестановок из* T *и если* $C(\sigma) \leqslant \sum_{i=1}^{n} C(\sigma_i)$, *то* σ *принадлежит* T.

Из утверждений (д. 1) и (д. 2) следует, что утверждение (д. 3) верно для $n = 1$ и $n = 2$. Сделаем индуктивное предположение, что утверждение (д. 3) справедливо для $n - 1$. В силу утверждения (д. 1), σ принадлежит T, если $C(\sigma) = C(\sigma_n)$; из нашего индуктивного предположения вытекает, что σ принадлежит T, если только $C(\sigma) \leqslant \sum_{i=1}^{n-1} C(\sigma_i)$. Допустим теперь, что $C(\sigma) \neq C(\sigma_n)$ и что $C(\sigma)$ не содержится в $K = \sum_{i=1}^{n-1} C(\sigma_i)$. Отсюда, в частности, следует, что и $C(\sigma_n)$ не содержится в K. Образуем прямую $C(\sigma) + C(\sigma_n) = L$; легко проверить, что $L \cap K$ будет точкой, отличной от $C(\sigma)$ и $C(\sigma_n)$. Согласно лемме 2, в группе Γ существует такая перестановка $\sigma' \neq 1$, для которой $C(\sigma') = L \cap K$; в силу нашего индуктивного предположения, σ' принадлежит T. Поскольку центр $C(\sigma)$ лежит на прямой $L = C(\sigma_n) + C(\sigma')$ и так как перестановки σ' и σ_n'' принадлежат T, то из утверждения (д. 2) следует, что и перестановка σ принадлежит T. Этим завершается индуктивное доказательство утверждения (д. 3).

Обозначим теперь через N сумму всех точек $C(\sigma)$, где σ пробегает все отличные от 1 элементы подгруппы T (в частности, если $T = 1$, то $N = 0$). Очевидно, что $T \leqslant \Gamma(N)$. Если σ — элемент подгруппы $\Gamma(N)$, то либо $\sigma = 1$, либо $C(\sigma) \leqslant N$. В последнем случае, в силу определения элемента N и аксиомы VII, существует

конечное число таких элементов $\sigma_1, \ldots, \sigma_n$ подгруппы T, что $C(\sigma) \leqslant \sum_{i=1}^{n} C(\sigma_i)$; но отсюда и из утверждения (д. 3) вытекает, что σ содержится в T. Таким образом, мы убедились, что $T = \Gamma(N)$, и этим утверждение (д) полностью доказано.

Замечание. Используя результаты, полученные в процессе предыдущих рассмотрений, читатель легко убедится в справедливости следующего интересного утверждения.

Если P — произвольная точка, не лежащая на гиперплоскости H, то каждый смежный класс группы Γ по подгруппе B содержит один и только один элемент из $\Gamma(P)$; мультипликативная группа отличных от 0 элементов тела F изоморфна группе $\Gamma(P)$.

§ 6. Теорема о представлении

Мы теперь закончили подготовку доказательства следующего основного результата настоящей главы.

Теорема. *Если частично упорядоченное множество S удовлетворяет аксиомам* I — IX *и если ранг максимального в S элемента M не меньше* 3, *то существует такое линейное многообразие (F, A), что S и частично упорядоченное множество $S(A)$ подпространств F-пространства A будут проективно эквивалентными.*

Доказательство. В силу теоремы о вложении и предложения 7 (§ 4), существует такое расширение T частично упорядоченного множества S, что T удовлетворяет аксиомам I — IX и M является в T гиперплоскостью. Максимальный элемент множества T мы обозначим через M'.

Образуем теперь группу $\Gamma(T, M)$ гиперплоскости M (см. § 5). Подгруппу группы $\Gamma(T, M)$, состоящую из всех перестановок σ, принадлежащих $\Gamma(T, M)$, центры которых содержатся в M, обозначим через A. В силу теоремы 1 (§ 5), A является абелевой группой. Через F обозначим совокупность всех таких эндоморфизмов η группы A, что $\Gamma(X)^{\eta} \leqslant \Gamma(X)$ для каждого $X \leqslant M$ (или, что эквивалентно, для каждого элемента X множества S), где через $\Gamma(X)$ обозначена подгруппа тех перестановок из A, центры которых содержатся в X. Из теоремы 1 (§ 5) следует, что F — тело, что подмножество V элементов из A тогда и только тогда является подпространством F-пространства A, когда $V = \Gamma(X)$ для некоторого X из S, и что отображение элемента X множества S на подпространство $\Gamma(X)$ из системы $S(A)$ всех подпространств F-пространства A определяет проективное отображение частично упорядоченного множества S на частично упорядоченное множество $S(A)$. Таким образом, построенное F-пространство A является требуемым линейным многообразием, представляющим наше частично упорядоченное множество S.

§ 7. Основы аффинной геометрии

Цель настоящего параграфа состоит в том, чтобы бегло показать связи между основами аффинной и проективной геометрий. Мы, в частности, покажем, что аффинную геометрию можно построить, опираясь лишь на результаты, изложенные в § 5, и что сравнительно более глубокая теорема о вложении (§ 4) для этой цели не нужна. В этом отношении проблема оснований аффинной геометрии является более простой, чем аналогичная проблема, относящаяся к проективной геометрии.

Прежде всего напомним, что каждое линейное многообразие (F, A) одновременно определяет и проективную и аффинную геометрии. Проективная геометрия, определяемая линейным многообразием (F, A), представляет собой частично упорядоченное множество $S(F, A)$ всех подпространств F-пространства A; *аффинная геометрия, определенная линейным многообразием* (F, A), *представляет собой частично упорядоченное множество* $V(F, A)$ *всех семейств* F*-пространства* A (см. гл. I, § 1). Семейством F-пространства A мы называем любое непустое подмножество W элементов из A, обладающее следующим свойством:

Если a, b, c — элементы из W и f — элемент тела F, то $f(a-b)+c$ принадлежит W.

Используя обычную терминологию теории групп, можно сказать, что семейства являются смежными классами F-пространства A по его подпространствам. Оказывается полезным следующее простое свойство семейств.

Лемма. *Непустое подмножество* W F*-пространства* A *в том и только в том случае является семейством, если элемент* $\sum_{i=1}^{n} f_i w_i$ *принадлежит* W *всякий раз, когда* w_i *— элементы из* W *и* f_i *— числа из* F, *удовлетворяющие условию* $\sum_{i=1}^{n} f_i = 1$.

Доказательство. Достаточность сформулированных условий почти очевидна. Пусть теперь W является семейством. Если элементы $w_1, \ldots, w_n$ принадлежат W и если числа f_i из F удовлетворяют условию $\sum_{i=1}^{n} f_i = 1$, то, очевидно,

$$w = \sum_{i=1}^{n} f_i w_i = \sum_{i=1}^{n-1} f_i (w_i - w_n) + w_n.$$

В силу основного свойства семейства, элемент $f_{n-1}(w_{n-1} - w_n) + w_n$ принадлежит W; отсюда, вновь используя основное свойство семейства, мы можем вывести, что к W принадлежит элемент $f_{n-2}(w_{n-2} - w_n) + f_{n-1}(w_{n-1} - w_n) + w_n$. Применяя теперь метод индук-

ции, нетрудно убедиться, что и само w принадлежит W; тем самым наша лемма полностью доказана.

Мы будем называть $V(F, A)$ *алгебраической моделью аффинной геометрии.* Сейчас мы проведем

Построение проективной модели аффинной геометрии. Для того чтобы это сделать, рассмотрим проективную геометрию S, которую мы можем представлять себе либо как систему $S(F, A)$ подпространств некоторого линейного многообразия (F, A), либо просто как частично упорядоченное множество S, удовлетворяющее аксиомам I — IX. Выделим в S некоторую гиперплоскость H. Тогда *аффинной геометрией* $[S, H]$ *будет частично упорядоченное множество всех тех элементов* (*или подпространств*) X *множества* S, *которые не содержатся в* H.

Употребляя обычную геометрическую терминологию, мы можем сказать, что аффинная геометрия $[S, H]$ возникает из проективной геометрии S при удалении из S гиперплоскости H («бесконечно удаленной» гиперплоскости).

Прежде всего заметим, что частичное упорядочение в множестве $[S, H]$ естественным образом индуцируется частичным упорядочением, определенным в S. Если Θ есть некоторое множество элементов из $[S, H]$, то ни один из элементов множества Θ не содержится в H; то же самое справедливо, очевидно, и для суммы элементов из Θ. Отсюда следует, что суммой элементов, принадлежащих $[S, H]$, будет вполне определенный элемент, также принадлежащий $[S, H]$. Но ситуация изменяется при переходе к рассмотрению пересечений. Действительно, если X и Y — элементы, принадлежащие $[S, H]$, то их пересечение $X \cap Y$ будет вполне определенным элементом из S. Однако $X \cap Y$ может быть частью гиперплоскости H; это никак не противоречит тому, что ни X, ни Y не содержатся в H. Следовательно, вполне возможно, что пересечения некоторой пары элементов из $[S, H]$ в $[S, H]$ не существует. Последнее обстоятельство на обычном геометрическом языке означает, что элементы X и Y аффинной геометрии $[S, H]$ параллельны.

Алгебраическое доказательство эквивалентности алгебраической и проективной моделей аффинной геометрии. Доказательству эквивалентности двух указанных моделей аффинной геометрии мы предпошлем следующие рассмотрения. Пусть (F, A) — линейное многообразие и H — его гиперплоскость. Тогда мы можем в F-пространстве A выбрать (причем различными способами) элемент t, не принадлежащий H; очевидно, что

$$A = H \dotplus Ft.$$

Если теперь X — некоторое подпространство F-пространства A, не содержащееся в гиперплоскости H, то обозначим через X^* совокупность таких элементов h из H, что $h + t$ принадлежит X. Мы покажем, что

(1) *X^* является семейством F-пространства A для каждого X из $[S(F, A), H]$.*

Доказательство. Так как подпространство X не содержится в H, то почти очевидно, что множество X^* не пусто. Если a, b, c — элементы из X^*, то a, b, c являются элементами гиперплоскости H, а элементы $a+t$, $b+t$, $c+t$ принадлежат X. Но X есть подпространство F-пространства A. Поэтому $(a+t)-(b+t)=a-b$ принадлежит $X \cap H$; отсюда вытекает, что если f — произвольное число из F, то $f(a-b)+(c+t)=[f(a-b)+c]+t$ будет элементом подпространства X. Следовательно, $f(a-b)+c$ принадлежит X^*, и этим показано, что X^* является семейством.

Из утверждения (1) следует, что отображение подпространства X из $[S(F, A), H]$ на X^* определяет однозначное и сохраняющее упорядочение отображение частично упорядоченного множества $[S(F, A), H]$ в частично упорядоченное множество $V(F, H)$.

Если теперь Y — произвольное семейство F-пространства H, то обозначим через Y^* подпространство F-пространства A, порожденное всеми элементами вида $y+t$, где $y \in Y$. Очевидно, что отображение Y в Y^* определяет однозначное и сохраняющее упорядочение отображение частично упорядоченного множества $V(F, H)$ в частично упорядоченное множество $[S(F, A), H]$. Построенные два отображения мы будем называть *звездными отображениями*; покажем, что

(2) *эти два звездных отображения взаимно обратны друг другу.*

Доказательство. Очевидно, что

$$Y \leqslant Y^{**} \text{ для каждого } Y \text{ из } V(F, H).$$

Пусть теперь z — произвольный элемент из Y^{**}. Тогда z является элементом гиперплоскости H, а $z+t$ принадлежит Y^*. Из определения подпространства Y^* следует существование таких элементов $y_1, \ldots, y_n$ из Y и таких чисел $f_1, \ldots, f_n$ из F, что

$$z+t=\sum_{i=1}^{n} f_i(y_i+t).$$

Поскольку элементы z и y_i принадлежат H и так как $A=H \dotplus Ft$, то из полученного равенства вытекает, что

$$z=\sum_{i=1}^{n} f_i y_i, \quad 1=\sum_{i=1}^{n} f_i.$$

Но отсюда и из леммы следует, что z принадлежит Y, ибо Y является семейством. Этим показано, что $Y=Y^{**}$.

Рассмотрим теперь некоторое подпространство X F-пространства A, не содержащееся в H. Нетрудно проверить, что X порождается элементами вида $t+x$, где x принадлежит X^*. Дру-

гими словами, подпространство X порождается множеством $t + X^*$; отсюда следует, что $X = X^{**}$. Наше же утверждение (2) по существу равносильно справедливости двух доказанных нами равенств $X = X^{**}$ и $Y = Y^{**}$.

Мы уже указали, что оба звездных отображения являются однозначными и сохраняющими частичное упорядочение. Используя теперь утверждение (2), легко убедиться, что наши звездные отображения являются, кроме того, взаимно однозначными и отображающими одно из множеств $V(F, H)$ и $[S(F, A), H]$ на все другое. Таким образом, эти отображения являются тем, что мы обычно называли проективными отображениями и что здесь лучше назвать аффинными отображениями. Полученный результат можно теперь сформулировать следующим образом:

(3) *Два звездных отображения определяют взаимно обратные аффинные соответствия между* $[S(F, A), H]$ *и* $V(F, H)$.

Теперь мы легко докажем эквивалентность алгебраической и проективной моделей аффинной геометрии. Предположим сначала, что нам дана некоторая алгебраическая модель $V(F, A)$ аффинной геометрии. Существует, очевидно, такое линейное многообразие (F, B), что A будет гиперплоскостью в (F, B). В F-пространстве B найдется такой элемент b, что $B = Fb + A$. Теперь можно построить звездное отображение частично упорядоченного множества $V(F, A)$ в частично упорядоченное множество $[S(F, B), A]$; в силу утверждения (3), это отображение определяет аффинную эквивалентность двух указанных множеств. Следовательно, $V(F, A)$ можно рассматривать и как проективную модель той же аффинной геометрии.

Пусть теперь нам дана некоторая проективная модель $[S, H]$ аффинной геометрии. Проективную геометрию S мы представим в виде ее алгебраической модели: $S = S(F, A)$, где (F, A) – соответствующим образом выбранное линейное многообразие. В таком случае H будет гиперплоскостью F-пространства A, и, следовательно, существует такой элемент t, что $A = Ft + H$. Построим теперь звездное отображение частично упорядоченного множества $[S(F, A), H]$ в частично упорядоченное множество $V(F, H)$; в силу утверждения (3), это отображение определяет аффинную эквивалентность двух указанных множеств. Следовательно, $[S, H] = [S(F, A), H]$ можно рассматривать и как алгебраическую модель аффинной геометрии; этим эквивалентность двух моделей аффинной геометрии полностью доказана.

Синтетическое построение алгебраических моделей аффинной геометрии. При построении алгебраической модели $V(F, H)$, эквивалентной данной проективной модели $[S, H]$ аффинной геометрии, мы предполагали, что проективная геометрия S дана нам в виде ее алгебраической модели $S(F, A)$. Другими словами, мы пользовались теоремой о представлении из § 6. Сейчас

мы хотим показать, что для того, чтобы построить алгебраическую модель аффинной геометрии, достаточно воспользоваться лишь рассмотрениями, проведенными в § 5, и что, следовательно, можно избежать использования теоремы о вложении из § 4.

Для того, чтобы это сделать, рассмотрим совокупность A всех автопроективных отображений σ проективной геометрии S, обладающих следующими свойствами:

(а) σ оставляет неподвижным каждый элемент из S, содержащийся в гиперплоскости H;

(б) σ обладает центром, принадлежащим H.

Из результатов § 5 следует, что A будет абелевой группой. Если X — подпространство, содержащееся в H, то через $\Gamma(X)$ обозначим совокупность элементов группы A, центры которых принадлежат X; совокупность эндоморфизмов η абелевой группы A, удовлетворяющих условию $\Gamma(X)^{\eta} \leqslant \Gamma(X)$ для каждого подпространства X, содержащегося в H, обозначим через F. В силу теоремы 1 (§ 5), F будет телом и отображение каждого подпространства X, содержащегося в гиперплоскости H, на подпространство $\Gamma(X)$ линейного многообразия (F, A) является проективным отображением частично упорядоченного множества подпространств проективной геометрии S, содержащихся в H, на систему $S(F, A)$.

Далее, выберем в S некоторую точку P, не принадлежащую гиперплоскости H. Если теперь X — произвольный элемент из $[S, H]$, то обозначим через X^* совокупность элементов σ группы A, отображающих точку P на точку, содержащуюся в X. Нетрудно проверить, что отображение элемента X на X^* устанавливает аффинную эквивалентность систем $[S, H]$ и $V(F, A)$; тем самым $V(F, A)$ является алгебраической моделью аффинной геометрии $[S, H]$. Детали доказательства мы оставляем читателю.

Внутренняя характеристика проективных моделей аффинной геометрии. Задача состоит здесь в том, чтобы охарактеризовать те частично упорядоченные множества L, которые аффинно эквивалентны проективной модели $[S, H]$ аффинной геометрии. Так как $L^* = [S, H]$ состоит из всех элементов проективной геометрии S, не содержащихся в H, то основная задача заключается в построении при помощи L^* тех элементов из S, которые являются частью гиперплоскости H. Этими элементами являются как раз так называемые идеальные элементы аффинной геометрии.

Основа для такого построения заложена, повидимому, в понятии M-структуры, введенном в работе Мак-Лейна [1]. Для построения идеальных элементов приходится развить теорию параллельности. Эта теория построена, например, в важной работе Менгера, на которую имеется ссылка в библиографическом указателе, помещенном в начале настоящей главы. (Заметим,

что часть энергии, сохраненной благодаря обходу теоремы о вложении, вкладывается в упомянутую теорию параллельности; однако, по мнению автора, несмотря на это, основы аффинной геометрии все же значительно проще основ проективной геометрии.)

Следует, кроме того, заметить, что синтетическое построение алгебраической модели аффинной геометрии, которое мы в общих чертах наметили выше, можно легко видоизменить таким образом, чтобы совершенно не использовать идеальных элементов (в то время, как мы все же ими пользовались); в связи с этим следует обратить внимание читателя на замечательную работу Артина, на которую имеется ссылка в библиографическом указателе, помещенном в начале настоящей главы.

ДОБАВЛЕНИЕ М

ОБЗОР ОСНОВНЫХ ПОНЯТИЙ И ПРИНЦИПОВ ТЕОРИИ МНОЖЕСТВ

В настоящий обзор мы намерены включить основные понятия теории множеств и формулировки результатов, относящихся к этим понятиям, не проводя никаких доказательств. Мы не будем касаться аксиом теории множеств и проблем, связанных с ними. Понятия и принципы теории множеств будут сформулированы в таком виде, который наиболее удобен для их применения; таким образом, наш обзор может быть полезен лишь как краткое собрание самых необходимых сведений из теории множеств. С основным же содержанием этой теории, которое находится вне нашего весьма поверхностного обзора, можно познакомиться по перечисленным ниже книгам:

Александров П. С.*, Введение в общую теорию множеств и функций, М.—Л., 1948.

Биркгоф Г. (Birkhoff G.), Теория структур, М., 1952.

Бурбаки (Bourbaci N.), Eléments de mathématiques, Actualités scient. et ind., 840, 858, 916, 934, 1029; Paris, 1939—1947.

Гёдель (Gödel K.), The Consistency of the Continuum Hypothesis, Ann. of Math. Studies, 3, Princeton.

Данжуа (Denjoy A.), L'énumération transfini, Paris, 1946.

Кавайес (Cavaillès J.), Transfini et continu, Paris, 1947.

Камке (Kamke E.), Allgemeine Mengenlehre, Enzyklopädie der math. Wiss., I, 1, 5.

Theory of Sets, New York, 1950.

Серпинский (Sierpinski W.), Leçons sur les nombres transfinis, Paris, 1928.

Hypothèse du continu, Warzsawa, 1934.

Тарский (Tarski A.), Cardinal Algebras, New York, 1949.

Френкель (Fränkel A.), Einleitung in die Mengenlehre, 3 Aufl., Berlin, 1928.

Хаусдорф Ф. (Hausdorff F.), Теория множеств, М.—Л., 1937.

Хермеш и Кёте (Hermes H. und Köthe G.), Die Theorie der Verbände, Enzyklopädie der math. Wiss., I, 1, 13.

МНОЖЕСТВА И ПОДМНОЖЕСТВА

Множество представляет собой произвольную совокупность элементов, которая либо может быть задана в совершенно абстрактном виде, либо составлена из некоторых специальных объектов другой природы подобно множествам точек, множествам чисел, множествам функций, множествам множеств и т. д.

Если S — некоторое определенное множество, то рассмотрим подмножества множества S. Это будут множества, все элементы которых принадлежат S. Совокупность подмножеств множества S имеет определенное математическое строение. Если U и V — подмножества множества S, то U может либо быть, либо не быть подмножеством множества V; в первом случае мы пишем $U \leqslant V$. Такое частичное упорядочение подмножеств множества S часто называют частичным упорядочением по включению.

Если Φ — некоторое множество подмножеств множества S, то пересечение $\prod_{X \in \Phi} X$ подмножеств, принадлежащих Φ, представляет собой совокупность всех элементов, каждый из которых принадлежит каждому подмножеству X из Φ; объединением, или суммой подмножеств, принадлежащих Φ, является совокупность элементов, каждый из которых принадлежит по крайней мере одному подмножеству из Φ.

ОТОБРАЖЕНИЯ

Если S и T — множества, то однозначное отображение σ множества S в множество T сопоставляет каждому элементу s из S однозначно определенный элемент (образ) s' из T. Образ элемента s при отображении σ обозначают различными способами (в соответствии с обстоятельствами), например $s\sigma$, s^{σ}, σs, $\sigma(s)$, ${}^{\sigma}s$ и т. д., а совокупность всех однозначных отображений множества S в множество T обозначается через T^S.

Однозначное отображение σ множества S в множество T называется отображением множества S *на* множество T, если каждый элемент из T является образом при отображении σ по крайней мере одного элемента из S.

Однозначное отображение σ множества S в множество T называется взаимно однозначным, если образы различных элементов из S различны.

Взаимно однозначные отображения множества S на множество T характеризуются тем свойством, что они обладают обратными отображениями; взаимно однозначные отображения множества S на себя называются перестановками множества S (независимо от того, конечно множество S или бесконечно).

ЧАСТИЧНО УПОРЯДОЧЕННЫЕ МНОЖЕСТВА

Множество S называется частично упорядоченным, если в нем определено соотношение «$\leqslant$», удовлетворяющее следующим условиям:

(а) Если a и b — элементы из S, то либо $a \leqslant b$, либо $b \leqslant a$, либо ни одно из этих соотношений не имеет места.

(б) $a \leqslant b$ и $b \leqslant a$ тогда и только тогда, когда $a = b$.

(в) Из $a \leqslant b$ и $b \leqslant c$ следует $a \leqslant c$.

Типичным примером частично упорядоченного множества является множество подмножеств данного множества S, упорядоченное по включению.

Если $a \leqslant b$, но $a \neq b$, то можно писать $a < b$ (ввиду условия (б)).

Каждое подмножество частично упорядоченного множества S само является частично упорядоченным множеством относительно того же соотношения упорядочения, которое определено в S. Подмножество T частично упорядоченного множества S называется *упорядоченным подмножеством множества* S, если оно удовлетворяет следующему условию:

(г) Для любых двух элементов a и b из T либо $a \leqslant b$, либо $b \leqslant a$.

Если T — некоторое подмножество частично упорядоченного множества S и u — такой элемент из S, что $t \leqslant u$ для каждого элемента t из T, то u называется *верхней гранью подмножества* T; аналогично определяются нижние грани. Элемент m из T называется *максимальным элементом подмножества* T, если из $m \leqslant t$, где t — элемент из T, следует $m = t$. (Заметим, что максимальные элементы не всегда являются верхними гранями.) Подобным же образом определяются минимальные элементы.

Мы теперь подготовлены к тому, чтобы сформулировать важный теоретико-множественный

Принцип максимального элемента. *Если каждое упорядоченное подмножество T частично упорядоченного множества S обладает верхней гранью, то каждое непустое подмножество T множества S обладает хотя бы одним максимальным элементом.*

Этот принцип впервые указал (в другой, но эквивалентной форме) Хаусдорф (см. книгу Хаусдорфа, упомянутую на стр. 382); см. также работу Уоллеса [1]. Применения указанного принципа рассматриваются в работах Тейхмюллера [1] и Цорна [1].

Наибольшее применение принцип максимального элемента находит при рассмотрении какого-либо множества S подмножеств (некоторого множества), упорядоченного по включению. Подмножество T множества S, к которому применим принцип макси-

мального элемента, обладает следующим свойством: если U — упорядоченное подмножество множества T, то объединение множеств, принадлежащих U, принадлежит T.

(Заменяя понятие верхней грани понятием нижней грани и максимальный элемент минимальным, мы получим принцип минимального элемента.)

Заметим, наконец, что взаимно однозначные отображения частично упорядоченных множеств, сохраняющие отношение порядка, называются проективными отображениями, а взаимно однозначные отображения, изменяющие отношение порядка на обратное, — дуальными отображениями.

ВПОЛНЕ УПОРЯДОЧЕННЫЕ МНОЖЕСТВА

Упорядоченное множество [т. е. множество, удовлетворяющее всем четырем условиям упорядочения (а) — (г)] называется вполне упорядоченным, если каждое его непустое подмножество обладает первым элементом. Знаменитая теорема Цермело утверждает, что каждое множество можно по крайней мере одним способом вполне упорядочить. Эта теорема эквивалентна принципу максимального элемента.

ПОРЯДКОВЫЕ ЧИСЛА

О двух вполне упорядоченных множествах S и T тогда и только тогда говорят, что они имеют одно и то же порядковое число, когда существует взаимно однозначное и сохраняющее упорядочение отображение множества S на множество T. Если существует взаимно однозначное и сохраняющее упорядочение отображение вполне упорядоченного множества S во вполне упорядоченное множество T, то говорят, что порядковое число множества S не превышает порядкового числа множества T. Если в данном произвольном множестве порядковых чисел определить только что указанным способом частичную упорядоченность, то в действительности это множество окажется вполне упорядоченным.

Если S — некоторое вполне упорядоченное множество, то каждый элемент s из S можно «занумеровать» порядковым числом множества элементов из S, предшествующих s. Это можно записать следующим образом:

$$S = \{s_0, s_1, \ldots, s_\nu, \ldots\}.$$

Каждое порядковое число ν обладает непосредственно следующим за ним порядковым числом, которое обозначают через $\nu + 1$. Однако существуют отличные от 0 порядковые числа, которые нельзя представить в таком виде; эти числа называются

предельными порядковыми числами. Первое предельное порядковое число обычно обозначают через ω; оно является порядковым числом множества целых положительных чисел при их естественном упорядочении.

Определение и доказательство методом трансфинитной индукции. Этот метод вполне аналогичен методу определения и доказательства при помощи полной математической индукции. Например, функция $f(\nu)$ определена для каждого порядкового числа ν, не превышающего σ, когда

(а) определено $f(0)$,

(б) указано правило нахождения значения $f(\nu+1)$, если известно значение $f(\nu)$,

(в) указано правило нахождения значения $f(\nu)$, где ν — предельное порядковое число, если известны значения функции $f(\tau)$ для каждого $\tau < \nu$.

Подобным же образом, утверждение $P(\nu)$ верно для каждого порядкового числа ν, не превышающего σ, если

(а) верно утверждение $P(0)$,

(б) утверждение $P(\nu+1)$ является следствием утверждения $P(\nu)$,

(в) утверждение $P(\nu)$, где ν — предельное порядковое число, справедливо в случае, когда верны утверждения $P(\tau)$ для каждого $\tau < \nu$.

Очень часто представляется возможным заменить доказательство методом трансфинитной индукции доказательством, использующим принцип максимального элемента; однако вопрос о том, каким из этих методов удобнее пользоваться, в различных случаях решается по-разному.

КАРДИНАЛЬНЫЕ ЧИСЛА

Говорят, что множества S и T имеют одно и то же кардинальное число, если между ними можно установить взаимно однозначное соответствие; кардинальное число множества S мы будем обозначать через $|S|$. Если существует взаимно однозначное отображение множества S в множество T, то говорят, что $|S| \leqslant |T|$. Можно доказать, что такая частичная упорядоченность кардинальных чисел в действительности будет полной упорядоченностью.

Бесконечные кардинальные числа обычно обозначают через $\aleph$. Первое из этих чисел обозначается через $\aleph_0$; оно является кардинальным числом множества целых чисел. Если S – произвольное множество, то кардинальное число множества всех подмножеств множества S обозначается через $2^{|S|}$. Знаменитая теорема Кантора утверждает, что

$$a < 2^a \text{ для каждого кардинального числа } a \neq 0.$$

Вопрос о том, справедливо или нет для каждого бесконечного кардинального числа равенство

$$2^{\aleph_\nu} = \aleph_{\nu+1},$$

пока остается открытым. Этот вопрос известен под названием «обобщенной проблемы континуума».

В то время как кардинальное число множества всех подмножеств больше кардинального числа исходного множества, ситуация изменяется при рассмотрении множества лишь некоторых специальных подмножеств данного множества. В связи с этим отметим следующую полезную теорему. Если S — бесконечное множество и если T — такое множество конечных подмножеств множества S, что каждый элемент из S принадлежит по крайней мере одному подмножеству из T, то $|T| = |S|$.

Алгебраические операции над кардинальными числами определяются следующим образом.

Сложение. Если a и b — кардинальные числа соответственно множеств A и B и если множества A и B не пересекаются, то $a + b$ является кардинальным числом объединения множеств A и B.

Умножение. Если a и b — кардинальные числа соответственно множеств A и B, то ab является кардинальным числом множества всех пар (x, y), где $x \in A$ и $y \in B$ (т. е. прямого произведения множеств A и B).

Возведение в степень. Если a и b — кардинальные числа соответственно множеств A и B, то a^b является кардинальным числом множества A^B всех однозначных отображений множества B в множество A. (Заметим, что это определение операции возведения в степень согласуется с нашим предыдущим определением кардинального числа 2^a.)

Законы поглощения. Если a и b — такие кардинальные числа, что $a \leqslant b$ и число b бесконечно, то

$$a + b = ab = b.$$

Дальнейшие сведения, относящиеся к алгебре кардинальных чисел, читатель может найти в указанной выше литературе.

ЛИТЕРАТУРА

Алберт (Albert A. A.)

[1] Modern Higher Algebra, Chicago, 1937.

[2] Structure of Algebras, Amer. Math. Soc. Coll. Pub., vol. 24, New York, 1939.

Анкочея (Ancochea G.)

[1] Le théorème de von Staudt en géométrie projective quaternionienne, Journal für die reine und angewandte Math., 184 (1942), 193—198.

Артин (Artin E.)

[1] Galois Theory, Notre Dame Math. Lectures, 2 (1944).

[2] The Influence of J. H. M. Wedderburn on the Development of Modern Algebra, Bull. Amer. Math. Soc., 56 (1950), 65—72, в частности 68—70.

Артин, Несбитт, Тролл (Artin E., Nesbitt C. J., Thrall R. M.)

[1] Rings with Minimum Condition, Ann. Arbor, 1944.

Артин, Уэйплс (Artin E., Whaples G.)

[1] The Theory of Simple Rings, Amer. Journal of Math., 65 (1943), 87—107.

Арф (Arf C.)

[1] Untersuchungen über quadratische Formen in Körpern der Charakteristik 2 (Teil I), Journal für die reine und angewandte Math., 183 (1941), 148—167.

Биркгоф (Birkhoff G.)

[1] Теория структур, М., 1952.

Биркгоф и Мак-Лейн (Birkhoff G., MacLane S.)

[1] A Survey of Modern Algebra, New York, 1948.

Биркгоф и Нейман (Birkhoff G., von Neumann J.)

[1] The Logic of Quantum Mechanics, Ann. of Math., 37 (1936), 823—843, в частности 837—843.

Бурбаки (Bourbaki N.)

[1] Eléments de mathématiques, Paris, 1937—1947.

Бэр (Baer R.)

[1] The Decomposition of Abelian Groups into Direct Summands, Quarterly Journal of Math., 6 (1935), 222—232.

[2] A Unified Theory of Projective Spaces and Finite Abelian Groups, Trans. Amer. Math. Soc., 52 (1942), 283—343.

[3] Automorphism Rings of Primary Abelian Operator Groups, Annals of Math. 44 (1943), 192—227.

[4] Free Mobility and Orthogonality, Trans. Amer. Math. Soc., 68 (1950), 439—460.
[5] The Group of Motions of a Two-Dimensional Elliptic Geometry, Compositio mathematica, 9 (1951), 271—288.
Ван-дер-Варден (van der Waerden B. L.)
[1] Gruppen von linearen Transformationen, Ergebnisse der Math., Bd. 4, 2, Berlin, 1935.
[2] Современная алгебра, тт. I, II, М.—Л., 1947.
Веблен и Янг (Veblen O., Young J. W.)
[1] Projective Geometry, vol. 1—2, 2nd ed. Boston, 1918—1938.
Вейль (Weyl H.)
[1] The Classical Groups, Princeton, 1946.
Витт (Witt E.)
[1] Theorie der quadratischen Formen in beliebigen Körpern, Journal für die reine und angewandte Math., 176 (1937), 31—48.
Вольфсон (Wolfson K. G.)
[1]* An Ideal-theoretic Characterization of the Ring of all Linear Transformations, Amer. Journal Math., 75 (1953), 358—386.
Джекобсон (Jacobson N.)
[1] Structure Theory of Simple Rings without Finiteness Assumptions, Trans. Amer. Math. Soc., 57 (1945), 228—245.
[2] Теория колец, М., 1947.
[3] Lectures in Abstract Algebra, vol. I, Basic Concepts, New York, 1951.
Джекобсон, Рикарт (Jacobson N., Rickart C. E.).
[1] Jordan Homomorphisms of Rings, Trans. Amer. Math. Soc., 69 (1950) 479—502.
Джонсон (Johnson R. E.)
[1] Equivalence Rings, Duke Math. Journal, 15 (1948), 787—793.
Дьёдонне (Dieudonné J.).
[1] Sur les groups classiques, Paris, 1948.
[2] On Automorphisms of the Classical Groups, Memoirs of the Amer. Math. Soc., No. 2, 1950.
[3] Sur les systèmes maximaux d'involutions conjuguées permutables dans les groupes projectifs, Summa Brasil. Math., 2 (1950), 59—94.
Дюбрей (Dubreil P.)
[1] Algèbre, t. 1, Paris, 1946.
Ефимов Н. В.
[1]* Высшая геометрия, М.—Л., 1945.
Кёте (Köthe G.)
[1] Schiefkörper unendlichen Ranges über dem Zentrum, Math. Ann., 105 (1931), 15—39.
Коксетер (Coxeter H. S. M.).
[1] The Real Projective Plane, New York, 1949.
Крулль (Krull W.)
[1] Elementare Algebra vom höheren Standpunkt, Berlin, 1939.

Курош А. Г.
[1]* Высшая алгебра, изд. 3, М.—Л., 1953.
Леви (Levi F.)
[1] Geometrische Konfigurationen, Leipzig, 1929.
[2] Algebra, Calcutta, 1942.
[3] Finite Geometrical Systems, Calcutta, 1942.
Магнус (Magnus W.)
[1] Allgemeine Gruppentheorie, Enzyklopädie der math. Wiss., I, 1, 9.
Мак-Даффи (MacDuffee C. C.)
[1] An Introduction to Abstract Algebra, New York, 1940.
[2] Vectors and Matrices, Corus Math. Monographs, 7, Ithaca, 1943.
Макки (Mackey G. W.)
[1] Isomorphisms of Normed Linear Spaces, Annals of Math., 43 (1942), 244—260.
Мак-Лейн (MacLane S. S.)
[1] A Lattice Formulation for Transcendence Degrees and p-Bases, Duke Math. Journal, 4 (1938), 455—468.
Мальцев А. И.
[1]* Основы линейной алгебры, М.—Л., 1948.
Менгер (Menger K.)
[1] The Projective Space, Duke Math. Journal, 17 (1950), 1—14.
Нейман (von Neumann J.)
[1] Continuous Geometry, Princeton, 1935—1937.
Пиккерт (Pickert G.)
[1] Einführung in die höhere Algebra, Studia Mathematica/Mathematische Lehrbücher, Bd. 7, Göttingen, 1951.
Поддерюгин В. Д.
[1]* Условие упорядочиваемости произвольного кольца, Успехи матем. наук, IX, вып. 4 (1954), 211—216.
Рейдемейстер (Reidemeister K.)
[1] Vorlesungen über Grundlagen der Geometrie, Berlin, 1930.
Рикарт (Rickart C. E.).
[1] Isomorphic Groups of Linear Transformations, I, Amer. Journal of Math., 72 (1950), 451—461.
[2] Isomorphic Groups of Linear Transformations, II, Amer. Journal of Math., 73 (1951), 697—716.
[3] Isomorphisms of Infinite Dimensional Analogues of the Classical Groups, Bull. Amer. Math. Soc., 51 (1951), 435—448.
Серре (Segre B.).
[1] Lezioni di geometria moderne, vol. 1, Fondamenti di geometria sopra un corpo qualsiasi, Bologna, 1948.
Селе (Szele T.)
[1]* On Ordered Skew Fields, Proc. Amer. Math. Soc., 3 (1952), 410—413.
Тейхмюллер (Teichmüller W.).
[1] Braucht der Algebraiker das Auswahlaxiom? Deutsche Mathematik, (1939), 567—577.

Титс (Tits J.)
[1] Généralisations des groupes projectifs, Acad. Roy. Belgique Bull., Cl. Sciences, 1949.
Уоллес (Wallace A. D.)
[1] A Substitute for the Axiom of Choice, Bull. Amer. Math. Soc., **50** (1944), 278.
Фринк (Frink O.)
[1] Complemented Modular Lattices and Projective Spaces of Infinite Dimension, Trans. Amer. Math. Soc., **60** (1946), 452—467.
Халмош (Halmos P.)
[1] Finite Dimensional Vector Spaces, Annals of Math. Studies, 7. Princeton, 1940.
Хассе (Hasse H.)
[1] Höhere Algebra, Bd. 1, 2; 2. Aufl., Berlin und Leipzig, 1933.
Хаупт (Haupt O.)
[1] Einführung in die höhere Algebra, Bd. 2, Leipzig, 1929.
Хермеш и Кёте (Hermes H., Köthe G.)
[1] Die Theorie der Verbände, Enzyklopädie der math. Wiss., I, 1, 13.
Ходж и Пидо (Hodge W. W. D., Pedoe D.)
[1] Методы алгебраической геометрии, т. 1, М., 1954.
Хуа Ло-гэн (Hua Loo-Keng).
[1] On the Automorphisms of the Symplectic Group over any Field, Annals of Math., 49 (1948), 739—759.
[2] On the Automorphisms of a Sfield, Proc. of the National Acad. of Sciences, 35 (1949), 386—389.
[3] Supplement to the Paper of Dieudonné on the Automorphisms of Classical Groups, Memoirs of the Amer. Math. Soc., No. 2, 1950.
Цассенхаус (Zassenhaus H.)
[1] The Theory of Groups, New York, 1949.
Цорн (Zorn M.)
[1] A Remark on Method in Transfinite Algebra, Bull. Amer. Math. Soc., **51** (1935), 667—670.
Чеботарев Н. Г.
[1]* Введение в теорию алгебр, М.—Л., 1949.
Четверухин Н. Ф.
[1]* Проективная геометрия, изд. 6, М., 1953.
Швердфегер (Schwerdtfeger H.)
[1] Introduction to Linear Algebra and the Theory of Matrices, Groningen, 1951.
Шмидт (Schmidt A.)
[1] Über die Bewegungsgruppe der ebenen elliptischen Geometrie, Journal fur die reine und angew. Math., 186 (1949), 230—240.
Шпернер (Sperner E.)
[1] Beziehungen zwischen geometrischer und algebraischer Anordnung, Sitzungsberichte der Heidelberger Akademie der Wissenschaften, Math.-nat. Kl., 1949 (10).
[2] Die Ordnungsfunktionen einer Geometrie, Math. Ann., 121 (1949), 107 и след.

[3] Einführung in die analytische Geometrie und Algebra, Teil I and 2, Studia Mathematica/Mathematische Lehrbücher, Bd. 1, 6, Göttingen, 1950.

Шрейер и Ван-дер-Варден (Schreier O., van der Waerden B. L.)

[1] Die Automorphismen der projektiven Gruppen, Abhandlungen aus dem mathematischen Seminar der Hamburgischen Universität, Bd. 6 (1928), 303—332.

Шрейер и Шпернер (Schreier O., Sperner E.)

[1] Einführung in die analytische Geometrie und Algebra, Bd. 1, 2, Leipzig und Berlin, 1931—1935.

Эссэр (Esser M.)

[1] Self-dual Postulates for n-Dimensional Projective Geometry, Duke Math. Journal, 18 (1951), 475—480.

УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ