НЕ СОВСЕМ НАИВНАЯ ЛИНЕЙНАЯ АЛГЕБРА
ЧАСТЬ 1:
МОДУЛИ И ЛИНЕЙНЫЕ ОТОБРАЖЕНИЯ

Николай Вавилов

Истину о трехмерном пространстве следует нести всем, даже женщинам и солдатам.

Эдвин Эббот, *Флатландия*, § 21

Все знают, как полезно быть полезным. Никто не знает, как полезно быть бесполезным.

Чжуан-цзы

Можно жить по вокзальным часам, а можно по солнечным.

Осип Мандельштам, *Египетская марка*

Во всех человеческих сообществах, во все времена, существует один процесс, который является показателем прогресса индивидуума или группы. Это рост глубины и изощренности понимания вещей.

Идрис Шах, *Знание как знать*

If you've been pounding nails with your forehead for years, it may feel strange the first time someone hands you a hammer. But that doesn't mean that you should strap the hammer to a headband just to give your skull that old familiar jolt. — Если Вы из года в год забивали гвозди лбом, Вы испытаете странное чувство, когда кто-то первый раз даст Вам в руки молоток. Но это не значит, что следует прибинтовывать молоток к голове просто для того, чтобы дать своему черепу привычную встряску.

Donald Knuth

Die Kunst will es von uns, daß wir nicht stehen bleiben. Sie werden eine neue Art der Stimmführung bemerken.— Искусство требует от нас, чтобы мы не стояли на месте. Вы заметите совершенно новый тип полифонии.

Ludwig van Beethoven

Каждый пишет, как он слышит.
Каждый слышит, как он дышит.
Как он дышит, так и пишет,
Не стараясь угодить ...
Так природа захотела.
Почему?
Не наше дело.
Для чего?
Не нам судить.

Булат Окуджава, *Я пишу исторический роман*

Жить в эпоху свершений, имея возвышенный нрав,
к сожалению, трудно.

Иосиф Бродский, *Конец прекрасной эпохи*

Оглавление

Введение

§ 1 ♢. Линейная алгебра 7
§ 2 ♠. Почему модули? 7
§ 3 ♠. Почему проективные модули? 11
§ 4 ♠. Почему левое $\neq$ правому? 12
§ 5 ♠. Двойственность 14
§ 6 ♠. Строки и столбцы 16
§ 7 ♠. Вы не врач — Вы вредитель 18
§ 8 ♡. Книги по линейной алгебре по-русски 19

Замысел конструктора 24

Глава 1. Модули 28

§ 1 ♢. Модули и векторные пространства 29
§ 2 ♢. Примеры модулей 32
§ 3 ♢. Свободные модули 34
§ 4 ♢. Линейные отображения 36
§ 5 ♠. Обратная замена кольца 38
§ 6 ♣. Прямая замена кольца 40
§ 7 ♢. Линейные комбинации 41
§ 8 ♢. Подмодули 42
§ 9 ♢. Линейная оболочка системы векторов 43
§ 10 ♢. Фактор-модуль 45
§ 11 ♢. Ядро и образ линейного отображения 46
§ 12 ♢. Теорема о гомоморфизме 47
§ 13 ♢. Сумма и пересечение подмодулей 48
§ 14 ♢. Прямые суммы и проекторы 50
§ 15 ♠. Прямые суммы и прямые произведения 52

Глава 2. Свободные и проективные модули 54

§ 1 ♢. Линейная зависимость и независимость 54
§ 2 ♢. Базис свободного модуля, координаты 55
§ 3 ♢. Формальные линейные комбинации 59
§ 4 ♢. Универсальное свойство базиса 59
§ 5 ♡. Единственность ранга 61
§ 6 ♠. Неединственность ранга 62
§ 7 ♢. Выделение подмодулей уравнениями на координаты 63
§ 8 ♠. Стабильно свободные модули 64
§ 9 ♢. Матрица перехода от базиса к базису 65
§ 10 ♢. Преобразование координат 66
§ 11 ♠. Координатные системы в проективных модулях 67

Глава 3. Векторные пространства 70

§ 1 ♢. Линейная зависимость над полем 70
§ 2 ♢. Теорема Штейница: доказательство методом замены 72

§ 3 ♢. Теорема Штейница: доказательство методом исключения .. 73
§ 4 ♢. Максимальные линейно независимые системы 74
§ 5 ♢. Минимальные системы образующих 75
§ 6 ♢. Существование базисов 77
§ 7 ♢. Размерность векторного пространства 78
§ 8 ♢. Относительный базис, коразмерность 80
§ 9 ♢. Теорема о размерности ядра и образа 81
§ 10 ♢. Теорема о размерности суммы и пересечения 83
§ 11 ♡. Векторные пространства над $\mathbb{F}_p$ 85
§ 12 ♡. Векторные пространства над $\mathbb{Q}$ 85
§ 13 ♡. Многочлены Гаусса 87
§ 14 ♡. Линейная алгебра над конечным полем 89

Глава 4. Линейная алгебра в классических примерах 91

§ 1 ♡. Пространства последовательностей 91
§ 2 ♡. Пространства функций: общие места 92
§ 3 ♡. Пространства функций: примеры 93
§ 4 ♡. Модули над кольцами функций 95
§ 5 ♡. Модули над кольцом многочленов 96
§ 6 ♡. Модули над кольцом дифференциальных операторов 96
§ 7 ♠. Пространство, порожденное сдвигами и растяжениями функции 97
§ 8 ♠. Интересные примеры линейной зависимости 99
§ 9 ♠. Теорема Дедекинда—Артина 100
§ 10 ♠. Топологические базисы 100

Глава 5. Линейные отображения 102

§ 1 ♢. Структура модуля на $\mathrm{Hom}_R(U, V)$ 102
§ 2 ♢. Структура алгебры на $\mathrm{End}_R(U)$ 105
§ 3 ♠. Функториальность 106
§ 4 ♢. Матрица линейного отображения 107
§ 5 ♢. Преобразование матрицы линейного отображения 108
§ 6 ♢. Линейные отображения прямых сумм 109
§ 7 ♡. Полулинейные отображения 110
§ 8 ♢. Диаграммы модулей и гомоморфизмов 111
§ 9 ♢. Неравенства Фробениуса и Сильвестра 114
§ 10 ♠. Фредгольмовы операторы 115
§ 11 ♠. Лемма о трех гомоморфизмах 117
§ 12 ♠. Лемма о пяти гомоморфизмах 119

Глава 6. Двойственность 120

§ 1 ♢. Двойственный модуль 120
§ 2 ♢. Преобразование координат ковектора 121
§ 3 ♢. Второе двойственное, двойственность 123
§ 4 ♢. Двойственное линейное отображение 124
§ 5 ♡. Двойственность для подмодулей 125
§ 6 ♡. Теорема Фредгольма 127

Остальные части курса:

Часть 2. Алгебра матриц
Часть 3. Инварианты и канонические формы матриц
Часть 4. Геометрическая алгебра
Часть 5. Полилинейная алгебра
Часть 6. Неравенства и выпуклый анализ

ВВЕДЕНИЕ

The man thinks. The horse thinks. The sheep thinks. The cow thinks. The dog thinks. The fish doesn't think, because the fish knows everything.

Goran Bregović

It is a common knowledge to every schoolboy and even to every Bachelor of Arts,
That all sin is divided into two parts.
One kind of sin is called a sin of commission, and that is very important,
And it is what you are doing when you are doing something you ortant,
And the other kind of sin is just the opposite and is called a sin of ommission and is equally bad in the eyes of all right-thinking people, from Billy Sunday to Buddha,
And it consists of not having done something you shuddha.

Ogden Nash, *Portrait of the artist as a prematurely old man*

Настоящая книга представляет собой запись лекций по линейной алгебре, которые я последние восемь лет читаю потоку прикладных математиков математико-механического факультета СПбГУ. Эта книга покрывает — с большим запасом! — весь материал, традиционно включаемый в курсы линейной алгебры, и, кроме того, во многих местах излагает дополнительный материал, представляющий точку зрения профессионального алгебраиста, возможные обобщения, вычислительные аспекты, а также иллюстрирующий приложения линейной алгебры.

§ 1♢. Линейная алгебра

В настоящее время линейная алгебра, в том смысле, как понимают этот термин современные математики, является наиболее широко используемым аппаратом для всех разделов чистой и прикладной математики — от теории алгебраических чисел до квантовой механики, не говоря уже о теории групп, алгебраической топологии и функциональном анализе. Одновременно обнаружилось, что логическая структура линейной алгебры исключительно проста и основывается на небольшом количестве удобных в обращении понятий и аксиом, хоть это и затушевывалось теми сложнейшими вычислениями с матрицами, определителями и тензорами с большим числом верхних и нижних индексов, которыми увлекались математики XIX века.

Жан Дьедонне

С моей точки зрения примерно так должен выглядеть *современный* учебник линейной алгебры для каждого, кто готовится к ее *серьезному* использованию, скажем, в рамках таких специальностей, как программирование, математическая экономика, теоретическая физика, квантовая химия, теория управления, кристаллография, информационные технологии, криптография и кодирование.

Дело в том, что действующие сегодня курсы линейной алгебры, читаемые экономистам и инженерам, полностью сформировались в докомпьютерную эпоху и основной упор в них обычно делается на отработку нескольких стандартных вычислительных приемов для пространств небольших размерностей, матриц небольших степеней, и т.д. По причинам, которые мы подробно обсуждаем в[1], БОЛЬШИНСТВО ЭТИХ ВЫЧИСЛИТЕЛЬНЫХ НАВЫКОВ В НАСТОЯЩЕЕ ВРЕМЯ ПОЛНОСТЬЮ ОБЕСЦЕНИЛИСЬ.

В связи с явной неадекватностью предлагаемых сегодня нематематикам математических курсов часто приходится слышать, что появление компьютеров делает вообще излишним серьезное изучение математики[2]. Нет ничего более далекого от истины! Очевидно, что именно в связи с резким ростом наших вычислительных возможностей математические курсы должны стать *гораздо* содержательнее и концептуальнее, а акцент в них должен быть перенесен с рутинных вычислений на развитие МАТЕМАТИЧЕСКОГО И АЛГОРИТМИЧЕСКОГО МЫШЛЕНИЯ И ФОРМИРОВАНИЕ ОБЩИХ ПОНЯТИЙ.

Как мы объясняем в следующих параграфах, предлагаемый в настоящей книге подход, основанный последовательном использовании модулей, в том числе над *некоммутативными* кольцами, и тщательном различении левых и правых модулей на уровне языка и обозначений, одновременно

• несравненно **эффективнее** в вычислительном отношении,

• гораздо **нагляднее** и проще для начинающего,

• значительно **содержательнее** с точки зрения как математических, так и экстра-математических приложений линейной алгебры,

• значительно **правильнее** с точки зрения профессионального алгебраиста,

чем изложения во всех традиционных учебниках линейной алгебры, написанных с **наивных** позиций. Настоящий учебник отличается от большинства обычных учебников линейной алгебры не только более общей точкой зрения, но и более широким охватом материала, значительно большим количеством математически интересных примеров и *гораздо* большим вниманием к деталям, в том числе вычислительным.

Дело в том, что большинство учебников **высшей алгебры** и **линейной алгебры** написаны людьми, которые матриц порядка больше, чем 3 или 4, сами никогда не умножали и поэтому просто не понимают возникающих при этом нюансов. Настоящий же текст, среди прочего, учитывает запросы курса “Математика и компьютер”, который В.Г.Халин и я вели послед-

---

[1] Н.А.Вавилов, В.Г.Халин, `Mathematica` 5.* для нематематика. Вып. 1. Первое знакомство. – ОЦЭиМ СПб, 2005, 1–180.

[2] В качестве дополнительного аргумента при этом выдвигается то, что математика уже полностью устранена из учебных программ в таких передовых странах, как Сингапур и Малайзия.

ние несколько лет на экономическом факультете СПбГУ. В сопровождающем его задачнике[3] содержатся задачи, где предлагается *реально* проделать *символьные* вычисления и *вычисления бесконечной точности* с матрицами, в которых несколько десятков, несколько сотен или даже несколько тысяч строк и столбцов.

С другой стороны, в отличие от подавляющего большинства книг по *вычислительной* линейной алгебре, предмет здесь рассматривается с чисто математической перспективы. Мы подчеркиваем принципиальные моменты и изложение сфокусировано *все же* на понимании, а не собственно вычислении. В частности, мы вообще не обсуждаем *приближенные* методы линейной алгебры, итеративные алгоритмы и большую часть тонкостей, связанных с практической организацией вычислений.

В первой главе мы начинаем изучать важнейший тип алгебраических систем — **модули** над кольцом. Модули над телами называются **векторными пространствами**. Вместе с каждым классом объектов естественно возникают морфизмы этих объектов, морфизмы модулей называются **линейными отображениями**. Изучение модулей, векторных пространств и линейных отображений как раз и называется **линейной алгеброй**.

Следующие шесть параграфов введения адресованы главным образом преподавателю. В них я излагаю свой взгляд на построение курса и некоторые принципиальные и технические аспекты. Недостатком настоящего учебника является не то, что я отхожу от традиций, сложившихся в преподавании линейной алгебры, а то, что я делаю это НЕДОСТАТОЧНО РАДИКАЛЬНО.

§ 2♠. Почему модули?

> Все знают, как полезно быть полезным. Никто не знает, как полезно быть бесполезным.
>
> Чжуан-цзы

> A large part of Mathematics which became useful developed with absolutely no desire to be useful.
>
> John von Neumann

Моя принципиальная позиция состоит в том, что в *любом* современном курсе линейной алгебры — даже в таком, который ориентирован в первую очередь на приложения! — ВСЕ ИЗЛОЖЕНИЕ ДОЛЖНО С САМОГО НАЧАЛА ВЕСТИСЬ НАД ПРОИЗВОЛЬНЫМИ КОЛЬЦАМИ, причем по возможности некоммутативными. Более того, даже для коммутативных колец следует тщательнейшим образом различать левые и правые модули. Сейчас мы приведем некоторые очевидные соображения в пользу такой неортодоксальной точки зрения.

---

[3] Н.А.Вавилов, В.Г.Халин, Задачи по курсу “Математика и компьютер”, Вып.4. Алгебра матриц. — ОЦЭиМ, СПб, 2008, 1–206.

• Даже за пределами самой алгебры недостаточно ограничиваться понятием векторного пространства. Дело в том, что в приложениях линейной алгебры в геометрии, (глобальном) анализе, теории дифференциальных уравнений, механике, физике, обычно приходится иметь дело не с векторами в какой-то точке, а с **векторными полями**. Векторные поля образуют модули над кольцами функций.

• С другой стороны, многие классы функций классического анализа не замкнуты относительно умножения. В то же время они замкнуты относительно сложения и выдерживают умножение на функции из различных колец функций и, таким образом, образуют модули над ними.

• Многие классы функций являются модулями над различными кольцами операторов, в частности, над кольцами дифференциальных операторов.

• Даже в самых классических приложениях речь обычно идет о матрицах с элементами из колец, скажем колец многочленов от одной или нескольких — коммутирующих или некоммутирующих! — переменных, различных колец функций или дифференциальных операторов.

• Многие современные приложения, связанные с передачей, хранением и обработкой информации, построением эффективных алгоритмов и т. д. требуют работы с целочисленными матрицами, матрицами с элементами из колец вычетов и других арифметических и конечных колец.

• Более того, даже если мы интересуемся только вычислениями с матрицами, элементы которых принадлежат некоторому полю, подавляющая часть эффективных современных алгоритмов основана на использовании блочной структуры, иными словами, представлении матриц над полем как матриц, элементы которых сами являются матрицами, т. е. объектами заведомо некоммутативными!

Это значит, что во всех доказательствах и вычислениях, всюду, где это не приводит к серьезным техническим трудностям, следует избегать ссылку на коммутативность основного кольца и приводить правильные *некоммутативные* формулы. Разумеется, МНОГИЕ ВОПРОСЫ ЛИНЕЙНОЙ АЛГЕБРЫ НАД НЕКОММУТАТИВНЫМ КОЛЬЦОМ СЛИШКОМ ТРУДНЫ ДЛЯ НАЧИНАЮЩЕГО: конечномерная линейная алгебра над некоммутативным кольцом включает в себя, как очень специальный частный случай, анализ бесконечномерной ситуации над полем, т. е. вопросы традиционно относящиеся к функциональному анализу!

Это значит, что при доказательстве большинства основных результатов приходится все же вводить различные упрощающие предположения, типа коммутативности или конечномерности. Тем не менее, стоит подчеркнуть, что большинство классических результатов не зависят от того, что основное кольцо R является полем, они справедливы в более общих ситуациях, если R коммутативно, либо является телом. Более того, ПРИ ПРОВЕДЕНИИ ДОКАЗАТЕЛЬСТВ В *естественной* ОБЩНОСТИ ИХ СТРУКТУРА ОБЫЧНО СТАНОВИТСЯ *гораздо* ПРОЗРАЧНЕЕ.

§ 3♠. Почему проективные модули?

Все лица выражали один тревожно-глубокомысленный вопрос: почем теперь фунт слоновьего мяса.

Осип Мандельштам, *Египетская марка*

Я считаю, что естественной общностью для развития линейной алгебры для начинающих является класс проективных модулей. Тем не менее, настоящий учебник построен более традиционно, большая часть содержательных результатов здесь доказывается только для свободных модулей.

• Как обычно, совершенно особую роль во всей теории играют универсальные объекты, в данном случае, модули, в которых существует **базис**. Такие модули называются **свободными**.

• Однако класс свободных модулей слишком узок для большинства приложений, как в самой алгебре, так и за ее пределами. Дело в том, что с геометрической точки зрения свободные модули соответствуют *тривиальным* расслоениям. В то же время естественную общность для развития линейной алгебры представляет класс **проективных** модулей, соответствующих *локально тривиальным* расслоениям. С чисто алгебраической точки зрения проективные модули — это в точности прямые слагаемые свободных.

• Проективные модули допускают адекватную вычислительную замену базисов — **координатные системы**. Все основные вычислительные процедуры линейной алгебры опираются не на линейную независимость базиса, а на линейность координат и, таким образом, легко обощаются на проективные модули.

Линейная алгебра над телом обладает рядом особенностей, резко упрощающих изучение векторных пространств по сравнению со случаем модулей над произвольным кольцом.

• Прежде всего, каждый модуль над телом свободен единственного ранга. Иными словами, в каждом векторном пространстве существует базис и любые два базиса состоят из одинакового количества элементов. Заметим, впрочем, что существование базиса в векторных пространствах представляет собой одну из эквивалентных формулировок аксиомы выбора.

Если ограничиться изучением свободных модулей, то существуют важные классы колец, для которых все подмодули свободного модуля свободны. Однако *только* тела обладают следующим удивительным свойством, которое собственно и определяет специфику линейной алгебры над телом.

• Каждое подпространство векторного пространства выделяется в нем прямым слагаемым. Иными словами, для любого подпространства $U \leq V$ существует **относительный базис**, так что в этом случае не только все подмодули, но и все фактор-модули свободных модулей свободны.

§ 4♠. Почему левое $\neq$ правому?

Невозможно понять, с какой стороны значение, с какой — знак ...
Поль Валери, *Тетради*

Элементарная линейная алгебра полна неясностей и противоречий. Каждый, кто пытается запомнить, как преобразуются при изменении базиса координаты геометрических объектов — ну хотя бы матрица линейного отображения — сталкивается с чудовищными трудностями. Трудности эти создаются на пустом месте, с единственной целью запугать и запутать студента.

• Например, почему-то коэффициенты матрицы a перехода от базиса к базису записываются слева, что приводит к **монструозным** текстам наподобие $v_j = \sum a_{ij} u_i$. Каждый, кто обладает хотя бы зачатками интеллекта и эстетического чувства, должен при виде такой формулы испытывать жесточайшие страдания и преодолевать мощнейшее психологическое сопротивление. Между тем, чтобы избавиться от подобной шизофрении, достаточно признать, что коэффициенты линейных комбинаций должны писаться *справа* от векторов — по крайней мере пока мы записываем функции слева от аргументов.

• Ну а уж, чтобы запомнить, что преобразуется при помощи a, что при помощи a^t, что при помощи a^{-1}, а что при помощи a^{-t}, об этом не приходится и говорить. Квалифицированный преподаватель обычно находится чуть в лучшем положении, обладая некоторым пониманием предмета и навыком вычислений он может вывести все нужные формулы у доски в реальном времени. Однако, подобному испытанию, причем без всякой необходимости, из чистого садизма подвергаются целые поколения студентов.

Все наивные учебники линейной алгебры не только грубо неправильны, но и прямо ошибочны. Дело в том, что следуя традиции их авторы не в состоянии или не желают различать левые и правые векторные пространства. Это порождает совершенно *чудовищные* тексты, при помощи которых потом невозможно провести ни одного конкретного вычисления. Пусть ϕ оператор, x вектор, а λ — скаляр. В большинстве обычных текстов собственные векторы определяются посредством $\phi(x) = \lambda x$, вместо правильного $\phi(x) = x\lambda$ — для *правых* собственных векторов — или $(x)\phi = \lambda x$ — для *левых* собственных векторов. Точно так же однородность выражается формулой $\phi(\lambda x) = \lambda\phi(x)$. В действительности для правых векторных пространств она должна записываться как $\phi(x\lambda) = \phi(x)\lambda$, а для левых векторных пространств — как $(\lambda x)\phi = \lambda(x)\phi$.

Подобное декадентство заведомо хуже *любого* профессионального подхода, как с позиции компетентного алгебраиста, так и с позиции квалифицированного прикладника или вычислителя. Разумеется, в отличие от авторов учебников, как профессиональный математик, так и профессиональный вычислитель обычно в состоянии легко отличить правое от левого.

С моей точки зрения даже для поля следует тщательнейшим образом различать левые и правые векторные пространства на уровне обозначений. Пространство столбцов K^n естественно рассматривать как *правое* векторное пространство, а двойственное к нему пространство строк ${}^nK$ — как *левое* векторное пространство. Конечно, в коммутативном случае более-менее безразлично, с какой стороны записывать скаляры, но тем не менее это различие имеет глубокий смысл: на правых векторных пространствах операторы действуют слева, а на левых векторных пространствах — справа[4]. А вот кольцо операторов некоммутативно, так что уже совсем не безразлично, с какой стороны записывать операторы!

В настоящей книге изложение ведется главным образом с точки зрения *правых* векторных пространств. В правых векторных пространствах скаляры действуют *справа*, а операторы — *слева*. Координаты вектора в правом векторном пространстве записываются *столбцами*, а базисы, соответственно, *строками*. С вычислительной точки зрения это означает, что как применение линейного отображения, так и выражение вектора в виде линейной комбинации представляет собой умножение столбца на матрицу *слева*.

При желании читатель может легко **транспонировать*** наше изложение на случай *левых* векторных пространств. При этом скаляры действуют *слева*, а линейные операторы — *справа*, координаты вектора записываются *строками*, а базисы, соответственно, *столбцами*. С вычислительной точки зрения это означает, что как применение линейного отображения, так и выражение вектора в виде линейной комбинации представляет собой умножение строки на матрицу *справа*.

Причины, по которым я строю изложение на основе правых векторных пространств носят не принципиальный, а чисто исторический и психологический характер. Во-первых, я привык к этому, так как писать столбец на доске удобнее, чем строку. Во-вторых, большинство потенциальных читателей этой книги являются правшами и придерживаются теоретико множественной точки зрения, согласно которой *отображения* записываются слева направо, а **компонуются*** справа налево. Иными словами, функция пишется *слева* от аргумента, например, $f(x)$, $\sin(x)$ и т.д.

Я считаю, что в изложении для начинающих было бы неправильно ориентироваться на более продвинутого читателя, который является левшой и придерживается теоретико категорной точки зрения, согласно которой *морфизмы* записываются справа налево, а компонуются слева направо. Тому, кто уже привык писать $(x)f$ и $(x)\mathrm{nis}$ — или, все же, $(x)\sin?$ — ничего не стоит перевести все результаты на свой язык.

Единственной небольшой трудностью последовательного применения на-

---

[4]И уж совсем удивительно поступает Лев Анатольевич Скорняков в книге “Элементы алгебры” (М., Наука, 1980, с.115), где как скаляры, так и операторы записываются справа. При этом он превращает правый R-модуль в правый же $\mathrm{End}(R)$-модуль. Разумеется, он компонует операторы слева направо, в обычных обозначениях $(\phi\psi)(x) = \psi(\phi(x))$, так что *в действительности* речь в его тексте идет о правом $\mathrm{End}(R)^o$-модуле.

*В музыкальном, а не в математическом смысле.

*`Компоновать` — образовывать композицию, `compose`. Многие профессионалы предпочитают более изысканное `компонировать` = `komponieren`.

шего подхода является вопрос о том, с какой стороны писать гомоморфизмы бимодулей! К сожалению, этот вопрос вообще невозможно решить до введения некоммутативных тензорных произведений!

§ 5♠. Двойственность

Поскольку бытие вещей заключается в их воспринимаемости, любая трансформация может происходить двумя путями — быть либо восприятием трансформации, либо трансформацией восприятия. Виктор Пелевин, *Настольная книга оборотня*

Связь между положением пятен Лауэ и истинным распределением узлов решетки в реальном пространстве должна определяться в соответствии со стереоскопическим проектированием: пятна Лауэ соответствуют узлам обратной решетки.

Анималу, *Квантовая теория твердых тел*

Не то блядь, не то московская кузина.

Александр Пушкин

Величайшее открытие XX века, которые некоторые приписывают Израилю Моисеевичу Гельфанду, а некоторые Александру Александровичу Гротендику, утверждает, что ФУНКЦИЯ ТАК ЖЕ СООТНОСИТСЯ С АРГУМЕНТОМ, КАК АРГУМЕНТ С ФУНКЦИЕЙ.

Конкретные манифестации этого принципа в линейной алгебре называются **двойственностью** или **альтернативой Фредгольма**. В простейшем виде двойственность утверждает, что векторы являются линейными формами на пространстве линейных форм, причем в конечномерном случае никаких других линейных форм на нем нет. Или, совсем по-простому, РЕШЕНИЯ СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ ТАК ЖЕ СООТНОСЯТСЯ С УРАВНЕНИЯМИ, КАК УРАВНЕНИЯ С РЕШЕНИЯМИ.

Этот принцип хорошо известен кристаллографам, физикам, инженерам, вычислителям и экономистам.

• В кристаллографии двойственность проявляется, например, в том, что картинка, которую мы видим при диффракции ренгеновских лучей на кристалле, отвечает не фактическому расположению атомов в кристалле, а узлам двойственной решетки. В кристаллографии различение роли векторов и ковекторов настолько важно, что систематически проводится на уровне терминологии. Специалист по физике твердого тела никогда не спутает зону Бриллюэна с ячейкой Вигнера—Зейтца (хотя с точки зрения математика и то и другое есть просто многогранник Вороного).

• Ярчайшей манифестацией двойственности является понятие канонических координат $q_1, \dots, q_n, p_1, \dots, p_n$ в гамильтоновом формализме, являющемся основой классической механики, да и вообще всей физики. А именно, уравнения Гамильтона—Якоби учат нас, что (с точностью до знака!) координаты $q_1, \dots, q_n$, так же относятся к импульсам $p_1, \dots, p_n$, как импульсы к координатам. В операторной интерпретации квантовой механики

q_i истолковывается как умножение на i-ю координату, а p_i — как дифференцирование по i-й координате. Однако, несмотря на изоморфизм между пространством векторов и пространством дифференцирований по направлениям

$$q_1\lambda_1 + \ldots + q_n\lambda_n \mapsto p_1\lambda_1 + \ldots + p_n\lambda_n,$$

физику не придет в голову отождествлять координаты с импульсами. Посмотрите, что происходит с $\dfrac{\partial}{\partial x_i}$ при замене переменных.

• Конкретным проявлением двойственности в квантовой механике является описание эволюции системы в картине Шредингера и в картине Гейзенберга, первая из которых соответствует восприятию трансформации, а вторая — трансформации восприятия. В формализме Дирака это проявляется как систематическое различение бра-векторов и кет-векторов.

• В теории кодирования имеется два основных способа задания кода, при помощи проверочной матрицы (уравнения) и при помощи порождающей матрицы (образующие). Снова, двойственность здесь настолько важна, что систематически отражается на уровне терминологии.

• Любой специалист по вычислительной математике прекрасно понимает различие левых и правых собственных чисел матрицы. Конечно, в коммутативном случае собственные числа матрицы и ее транспонированной совпадают. Но это совершенно не значит, что их фактическое нахождение представляет собой одну и ту же *вычислительную* задачу!

• Еще одна область, в которой двойственность играет огромную роль, это выпуклый анализ и линейное программирование. Важнейшие алгоритмы оптимизации прямо основаны на использовании двойственности.

Таким образом, *все* реальные приложения линейной алгебры показывают необходимость тщательно различать пространство и двойственное пространство. Если исходное пространство расматривается как *правое* векторное пространство, то двойственное пространство должно рассматриваться как *левое* векторное пространство, и наоборот. Таким образом, векторное пространство никогда не может быть *естественно* изоморфно своему двойственному. Это один из многих примеров, когда специалисты в прикладных областях придерживаются подхода, который даже с чисто математической точки зрения — именно с чисто математической точки зрения! — гораздо глубже и правильнее, чем то, что предлагают традиционные учебники линейной алгебры,

Таким образом, вопрос о том, с какой стороны записывать гомоморфизмы левых модулей, имеет не чисто академическое значение. А именно, обычно отображение $V \longrightarrow V^{**}$, $x \mapsto x^{**}$, модуля во второй двойственный определяется так: $x^{**}(f) = f(x)$. Но в этих обозначениях никакой двойственности не получается, нужны не две, а целых четыре звездочки, чтобы вернуть элемент x where it belongs. Правильная формула выглядит так: $(f)x^{**} = f(x)$.

Посмотрите, что происходит в гамильтоновом формализме, когда векторы (координаты) и ковекторы (импульсы) рассматриваются как принадлежащие одному и тому же (правому) векторному пространству. Появляющийся в уравнениях Гамильтона—Якоби знак -1 как раз и служит конкретным выражением того, что в этом случае тождественным отображением является не вторая, а лишь *четвертая* степень изоморфизма $x \mapsto x^*$.

§ 6♠. Строки и столбцы

> Everything you've learned in school as "obvious" becomes less and less obvious as you begin to study.
>
> R. Buckminster Fuller

Я привык изображать *векторы* (векторы!) *столбцами*, а *ковекторы* (функционалы, линейные формы, линейные уравнения, ...) — *строками*. В этом случае физик сказал бы, что векторы это *кет-векторы*, а ковекторы — это *бра-векторы*. Разумеется, возможна и другая точки зрения, согласно которой векторы изображаются строками, а ковекторы — столбцами, однако при этом ковектор должен писаться *справа* от вектора, нак котором он действует!

Транспонирование создает *опасную иллюзию* того, что K^n естественно изоморфно ${}^nK$. В действительности, этот изоморфизм совершенно не является естественным.

• Во-первых, в случае некоммутативного кольца без дополнительной структуры (такой, скажем, как инволюция), никакого изоморфизма R^n и ${}^nR$ нет. Есть изоморфизм между R^n и ${}^n(R^o)$.

• Во-вторых, даже в коммутативном случае изоморфизм $R^n \longrightarrow {}^nR$, $v \mapsto v^t$, зависит от выбора стандартных базисов строк и столбцов.

• Во-третьих, зафиксировав изоморфизм $K^n \longrightarrow {}^nK$, $v \mapsto v^t$, мы задаем на K^n сильнейшую *дополнительную* структуру, эвклидово скалярное произведение.

• В-четвертых, ценой подобной неряшливости является утрата способности ясно различать пространство и его двойственное и усложнение многих формул.

• И, наконец, если уж и задавать какой-то изоморфизм между пространствами столбцов и строк, то столбцу

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

нужно ставить в соответствие вовсе не **транспонированную** строку

$$(x_1, \dots, x_n),$$

а **полярную** строку

$$(x_n, \dots, x_1).$$

• Сопоставив столбцу транспонированную строку, мы сразу становимся на вещественную точку зрения — разумеется, классики так и поступали! Однако, сделав это мы начинаем заниматься эвклидовой геометрией, а вовсе не линейной алгеброй. Иными словами, изучать инварианты (классической) ортогональной группы, а не полной линейной группы!

• С точки зрения теории представлений действия полной линейной группы $\mathrm{GL}(n, R)$ на строках и столбцах **контраградиентны**. Это значит, что в то время как положительное направление на строках слева направо, положительное направление на столбцах — снизу вверх. По крайней мере одно из них приходит в противоречие с традициями европейского — и китайского! — письма. Транспонирование переводит верхнюю треугольную матрицу, действующую в *положительном* направлении, в нижнюю треугольную матрицу, действующую в *отрицательном* направлении. Тем самым, если мы хотим получить *настоящее* соответствие между столбцами и строками в линейной алгебре, мы должны после транспонирования снова заставить матрицу действовать в положительном направлении. Этого можно добиться, *например*, снова сделав матрицу верхней треугольной при помощи сопряжения. Таким образом, *настоящее* соответствие между строками и столбцами в линейной алгебре обеспечивается не обычным транспонированием, а транспонированием относительно побочной диагонали.

• Последовательное применение этого принципа затрагивает все возникающие в линейной алгебре формулы. Например, если при приведении по строкам ступенчатый вид матрицы x равен

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

то при приведении транспонированной матрицы x^t по столбцам этому соответствует вовсе не матрица

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

как получалось бы при транспонировании, а матрица

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

Совершенно замечательно, что в 206 году до н. э. китайские товарищи понимали это значительно глубже и правильнее, чем авторы современных учебников линейной алгебры, и приводили матрицу системы именно к такому виду!

§ 7♠. Вы не врач — Вы вредитель.

Not only is this incomprehensible, but the ink is ugly and the paper is from the wrong kind of tree.

Referees' Report, anonimous

Преподавание линейной алгебры отягощено традицией почти в такой же степени, как преподавание математического анализа. Структура существующих курсов в основных чертах сложилась в конце XIX века. В то время многие авторы стояли на чисто вещественной точке зрения и не отличали абстрактное векторное пространство от векторного пространства с дополнительной структурой. А именно, они обычно снабжали векторные пространства эвклидовым скалярным произведением $(u, v) = u^t v$. При помощи этого скалярного произведения они отождествляли пространство столбцов K^n с пространством строк ${}^nK$.

В традиционных учебниках любят давать ничего не говорящие вычислительные доказательства самых простых результатов. Используемые в них рассуждения *имитируют* принятые в математике способы рассуждений, но при этом вводится громадное количество не относящихся к делу обозначений и вычислительных деталей, единственная цель которых состоит в том, чтобы создать впечатление глубокомыслия и сложности и как можно больше запутать студента.

Например, вместо того, чтобы обозначать матрицы одной буквой — ровно для этого матрицы и вводились! — рисуются матрицы громадных порядков, с большим количеством многоточий. Встаньте на место студента и попробуйте в таких обозначениях понять, что такое, например, матрица Сильвестра. Гораздо полезнее было бы не громоздить многоэтажные многоточия, а просто нарисовать матрицу Сильвестра для многочленов степени 2 или 3 — именно так я стараюсь поступать в настоящей книге.

Для полного реализма в нескольких местах наряду с настоящим *математическим* доказательством под заголовком `имитация доказательства` я воспроизвожу подобное *учебное* доказательство. Эти псевдодоказательства приведены с тем, чтобы — уже понимая суть дела — студент мог изучить повадки писателей в области линейной алгебры.

Ну а уж рассказывать, как это делается в [IP], в первом семестре с бессодержательными чисто калькулятивными доказательствами такие вещи, как теорема Лапласа или теорема Бине—Коши ПРЕДСТАВЛЯЕТ СОБОЙ ПРЯМОЕ ВРЕДИТЕЛЬСТВО*. В третьем семестре, после введения понятия внешнего произведения, это можно будет сделать с доказательством, занимающим несколько строк и, главное, *естественным*.

К сожалению, традиции преподавания линейной алгебры оторваны как от практики серьезной математики, так и от настоящей вычислительной практики. Между тем, линейная алгебра представляет собой живую науку. Просто сегодня эта наука обычно называется теорией модулей, теорией представлений, гомологической алгеброй, алгебраической K-теорией и т.д. Однако, существующие учебники линейной алгебры не учитывают ни изменившееся за последние 80 лет понимание алгебры, ни современные обозначения и терминологию, ни фактический прогресс во многих направлениях, ни неожиданные, а часто просто совершенно ошеломительные приложения, ни даже возникшие в последние десятилетия совсем короткие и простые доказательства большинства классических теорем!

С другой стороны, в нынешнем виде многие курсы линейной алгебры абсолютно бесполезны (а часто и прямо вредны!) при проведении практических вычислений. Дело в том, что они не учитывают произошедшее за последние 50 лет изменения наших вычислительных возможностей — и потребностей. Излагаемые в них алгоритмы относятся к эпохе, предшествующей строительству египетских пирамид, и большинство из них невозможно использовать для фактических вычислений с матрицами размера 5×5. Лет 20 назад мне встречались студенты, которые после прослушивания курса линейной алгебры пытались решать системы линейных уравнений или обращать матрицы с использованием определителей, в то время как единственный случай, когда матрицу можно обращать таким способом, это матрицы 2×2. Сегодня подобное эпическое мракобесие встречается реже. Однако, авторы *элементарных* учебников по-прежнему убеждены сами и пытаются убедить студента, что системы линейных уравнений фактически решаются методом Гаусса!

§ 8♡. Книги по линейной алгебре по-русски

> Cette répétition continuelle de combats qui se ressemblent tous, ces dieux qui agissent toujours pour ne rien faire de décisif, cette Hélène qui est le sujet de la guerre, et qui à peine est une actrice de la pièce; cette Troie qu'on assiège et qu'on ne prend point, tout cela me causait le plus mortel ennui. J'ai demandé quelquefois à les savantes s'ils s'ennuyaient autant que moi à cette lecture: tous le gens sincères m'ont avoué que le livre leur tombait des mains.
>
> Voltaire, *Candide ou l'optimisme*

*Вы не врач — Вы вредитель! — Русско-китайский разговорник.

Литература по линейной алгебре необозрима. С одной стороны, это *огромное* количество *элементарных* учебников, которые говорят одно и то же одними и теми же словами. Книги эти по своим органолептическим качествам и питательной ценности напоминают плохо пережеванный картон. С другой стороны, это *огромное* количество высоко специализированных текстов по *специфическим* вычислительным аспектам линейной алгебры и некоторым ее приложениям.

Книг же, которые могли бы сообщить начинающему подлинное *математическое* понимание основных сторон предмета, совсем мало. Вот некоторые источники, которые представляются мне наиболее полезными — во всяком случае, сам я смог узнать из каждого из них что-то новое.

• **Учебники линейной алгебры:** [KM], [Ko2], [Ge], [Ha], [St], [Pr]. С *огромным* отрывом лучшим учебником общего характера на русском языке продолжает оставаться книга Кострикина и Манина [KM], также ее облегченный вариант [Ko2]. Книги Гельфанда [Ge] и Халмоша [Ha] написаны давно, примерно полвека назад, но с *ослепительной* ясностью. Поэтому они хорошо смотрятся и сегодня. Книга Прасолова [Pr] рассчитана на очень сильного или мотивированного студента, несмотря на маленький объем, в ней приведены короткие концептуальные доказательства большинства ключевых фактов. Ориентированный на инженеров и экономистов учебник Стренга [St] гораздо более элементарен. Многие основные результаты доказываются там только над вещественным полем, зато приводится огромное количество простых примеров. Из *совсем* элементарных учебников, содержащих детальный разбор стандартных примеров, типа тех, которые обычно дают в контрольных работах, можно рекомендовать [BLT], [Bo], [Go].

• **Учебники алгебры:** [Ko1], [Vi], [F]. Линейной алгебре в них посвящены короткие главы, но отдельные темы изложены там лучше или иначе, чем в других источниках. Например, в книге Фаддеева [F] содержится чрезвычайно доступное изложение внешней алгебры, а в книге Винберга [Vi] приводятся основанные на линейной зависимости доказательства основных фактов об определителях, которые работают только над полем, но зато гораздо короче обычных вычислительных доказательств.

• **Задачники:** [Ik1], [Zad], [PR], [FS]. Вот уже несколько десятилетий как основной в СПбГУ используется задачник Фаддеева и Соминского [FS]. Впрочем, это задачник *промежуточного* уровня, в [Pr] и [Ik1] можно найти гораздо больше стандартных вычислительных задач, а в [Zad] — более трудные задачи.

• **Вычислительная линейная алгебра:** [GVL], [De], [Pa], [Pi], [VK], [Wi], [FF]. Имеется громадное количество книг по различным вопросам вычислительной линейной алгебры, но большинство из них *слишком* специальны. Классическая книга Д.К.Фаддеева и В.Н.Фаддеевой [FF] содержит очень ясно написанное теоретическое введение и исчерпыающее изложение методов, развитых в докомпьютерную эпоху. Книга В.В.Воеводина и Ю.А.Кузнецова [VK] представляет собой очень удачный справочник. Там нет никаких доказательств и довольно мало примеров, но собраны и систематизированы многие сотни определений и фактов. Из учебников, содержащих фактические алгоритмы, [GVL] и [De] показались мне самыми полезными и понятными.

• **Теория матриц:** [Be], [Ga], [JS], [La], [HJ], [MM]. Самым полезным и основательным среди наивных изложений теории матриц на русском языке явдяется книга Хорна и Джонсона [HJ]. Среди книг, рассчитанных на инженеров, наиболее удачной кажется мне книга Ланкастера [La]. При весьма скромном объеме она содержит большой фактический материал и дает правильную трактовку многих принципиальных вопросов, что является большой редкостью в наивных изложениях. Замечательные книги [Be] и [JS] концентрируется на приложениях. Книга Гантмахера [Ga] основательно устарела в том, что касается обозначений и, чтобы ее читать, нужно уже знать все, что в ней написано и иметь много свободного времени. Однако, в этом случае в ней можно найти много интересного. В справочнике Маркуса и Минца [MM] нет доказательств, но упомянуто огромное количество полезных фактов.

• **Более продвинутые тексты:** [Ar], [Ba], [Bou1], [Bou2], [Co], [L], [Mi], [MH], [Sh], [Fa]. В перечисленных книгах линейная алгебра трактуется с точки зрения профессионального алгебраиста — т.е. над произвольным телом или даже над произвольным ассоциативным кольцом. Самой доступной из них является маленький шедевр Артина [Ar], самой основательной — монография Фейса [Fa]. Учебники Ленга [La] и Бурбаки [Bou1], [Bou2] несколько проще и в то же время содержат достаточно полное изложение основных вопросов. Книга Шафаревича [Sha] не является учебником в обычном смысле, она объясняет *смысл* основных понятий алгебры и их роль за ее пределами. Книга Кона [Co] специально посвящена особенностям некоммутативной ситуации.

[Al] П. С. Александров, *Курс аналитической геометрии и линейной алгебры*, Наука, М., 1979, 512с.

[Ar] Э. Артин, *Геометрическая алгебра*, Наука, М., 1990, 318с.

[AHU] А. Ахо, Дж. Хоркрофт, Дж. Ульман, *Построение и анализ численных алгоритмов*, Мир, М., 1979, 536с.

[Ba] Х. Басс, *Алгебраическая K-теория*, Мир, М., 1973, 591с.

[Be1] Д. В. Беклемишев, *Дополнительные главы линейной алгебры*, Наука, М., 1983.

[Be2] Д. В. Беклемишев, *Курс аналитической геометрии и линейной алгебры*, Наука, М., 1985.

[APCh] Л. А. Беклемишева, А. Ю. Петрович, И. А. Чубаров, *Сборник задач по аналитической геометрии и линейной алгебре*, Наука, М., 1987, 496с.

[Be] Р. Беллман, *Введение в теорию матриц*, Наука, М., 1976, 351с.

[BLT] Э. Л. Блох, Л. И. Лошинский, В. Я. Турин, *Основы линейной алгебры и некоторые приложения*, Высшая школа, М., 1971, 256с.

[Bo] З. И. Боревич, *Определители и матрицы*, Наука, М., 1988, 184с.

[Bô] М. Бохер, *Введение в высшую алгебру*, ГТТИ, М.–Л., 1933, 291с.

[BP] В. С. Булдырев, Б. С. Павлов, *Линейная алдгебра. Функции многих переменных*, Изд-во ЛГУ, Л., 1985, 496с.

[Bou1] Н. Бурбаки, *Алгебра, Гл.* I – III. *Алгебраические структуры, линейная и полилинейная алгебра*, Наука, М., 1962, 516с.

[Bou2] Н. Бурбаки, *Алгебра, Гл.* VII – IX. *Модули, кольца, формы*, Наука, М., 1966, 555с.

[Bou3] Н. Бурбаки, *Алгебра, Гл.* X. *Гомологическая алгебра*, Наука, М., 1987, 182с.

[Bae] Р. Бэр, *Линейная алгебра и проективная геометрия*, НИЛ, М., 1955, 399с.

[vdW] Б. Л. ван дер Варден, *Алгебра*, Наука, М., 1976, 648с.

[Vi] Э. Б. Винберг, *Курс алгебры*, Наука, М., 1999, 527с.

[Vo1] В. В. Воеводин, *Вычислительные основы линейной алгебры*, Наука, М., 1977, 303с.

[Vo2] В. В. Воеводин, *Линейная алгебра*, Наука, М., 1980.

[VK] В. В. Воеводин, Ю. А. Кузнецов, *Матрицы и вычисления*, Наука, М., 1984, 318с.

[G] Ф. Р. Гантмахер, *Теория матриц, 2-е изд.*, Наука, М., 1966.

[Ga] С. И. Гасс, *Линейное программирование. Методы и приложения*, Физматгиз, М., 1961.

[Ge] И. М. Гельфанд, *Лекции по линейной алгебре, 5-е изд.*, Наука, М., 1998, 272 с.

[GL] И. М. Глазман, Ю. И. Любич, *Конечномерный линейный анализ*, Наука, М., 1969, 475с.

[Go] Л. И. Головина, *Линейная алгебра и некоторые ее приложения. 4-е изд.*, Наука, М., 1985, 392с.

[GvL] Дж. Голуб, Ч. Ван Лоун, *Матричные вычисления*, Мир, М., 1999.

[GK] Р. Грегори, К. Кришнамурти, *Безошибочные вычисления. Методы и вычисления*, Мир, М., 1988, 208с.

[Da] Дж. Данциг, *Линейное программирование, его обобщения и применения*, Прогресс, М., 1966, 600с.

[De] Дж. Деммель, *Вычислительная линейная алгебра*, Мир, М., 2001, 429с.

[JS] Г. Джеффрис, Б. Свирлс, *Методы математической физики. Т.1*, Мир, М., 1969, 423с.

[JL] А. Джордж, Дж. Лю, *Численное решение больших разреженных систем уравнений*, Мир, М., 1984.

[Di1] Ж. Дьедонне, *Линейная алгебра и элементарная геометрия*, Наука, М., 1972, 334с.

[Di2] Ж. Дьедонне, *Геометрия классических групп*, Мир, М., 1974, 204с.

[ER] Н. В. Ефимов, Э. Р. Розендорн, *Линейная алгебра и многомерная геометрия*, Наука, М., 1974, 544с.

[Zad] *Задачи по алгебре. Вып. 3. Линейная алгебра*, Изд-во СПбГУ, 2003, 51с.

[Ik1] И. Х. Икрамов, *Задачник по линейной алгебре*, Наука, М., 1975.

[Ik2] И. Х. Икрамов, *Численное решение матричных уравнений*, Наука, М., 1984, 190с.

[IK3] И. Х. Икрамов, *Численные методы для симметричных линейных систем*, Наука, М., 1988, 159с.

[IP] В. В. Ильин, Э. Г. Позняк, *Линейная алгебра*, Наука, М., 1974, 296с.

[KFA] Р. Калман, П. Фарб, М. Арбиб, *Очерки по математической теории систем*, УРСС, М., 2004, 400с.

[KE] А. Картан, С. Эйленберг, *Гомологическая алгебра*, ИИЛ, М., 1960, 510с.

[Ka] Ф. Каш, *Модули и кольца*, Мир, М., 1981, 368с.

[K1] Д. Э. Кнут, *Искусство программирования. Т.* I, *Основные алгоритмы, 3-е изд*, Вильямс, М.–СПб–Киев, 2000, 712с., см. с.49, 111.

[K2] Д. Кнут, *Искусство программирования. Т.* II. *Получисленные алгоритмы*, Вильямс, М.–СПб.–Киев, 2000, 828с.

[Co] П. Кон, *Свободные кольца и их связи*, Мир, М., 1975, 422с.

[Ko1] А. И. Кострикин, *Введение в алгебру,* I. *Основы алгебры*, Физматлит, М., 2000.

[Ko2] А. И. Кострикин, *Введение в алгебру,* II. *Линейная алгебра*, Физматлит, М., 2001, 367с.

[KM] А. И. Кострикин, Ю. И. Манин, *Линейная алгебра и геометрия, 2е изд.*, Наука, М., 1986, 303с.

[Lam] И. Ламбек, *Кольца и модули*, Мир, М., 1971, 279с.

[La] П. Ланкастер, *Теория матриц*, Наука, М., 1978, 280с.

[Lan] К. Ланцош, *Практические методы прикладного анализа*, ГИФМЛ, М., 1961, 524с.

[L] С. Ленг, *Алгебра*, Мир, М., 1968, 564с.

[Lin] *Линейные неравенства и смежные вопросы*, ИИЛ, М., 1959, 469с.

[MWS] Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн, *Теория кодов, исправляющих ошибки*, Связь, М., 1979, 744с.

[M] С. Маклейн, *Гомология*, Мир, М., 1966, 543с.

[Ma] А. И. Мальцев, *Основы линейной алгебры*, Наука, М..

[MM] М. Маркус, Ч. Минк, *Обзор по теории матриц и матричных неравенств*, Наука, М., 1972, 232с.

[Mi] Дж. Милнор, *Введение в алгебраическую K-теорию*, Мир, М., 1974, 196с.

[MH] Дж. Милнор, Д. Хьюзмоллер, *Симметрические билинейные формы*, Наука, М., 1986, 176с.

[MTTF] М. В. Милованов, М. М. Толкачев, Р. И. Тышкевич, А. С. Феденко, *Алгебра и аналитическая геометрия. Части* I, II, Вышейшая Школа, Минск, 1984; 1987.

[MP] А. П. Мишина, И. В. Проскуряков, *Высшая алгебра. Линейная алгебра, многочлены, общая алгебра*, ГИФМЛ, М., 1962, 300с.

[Mu] Б. Муртаф, *Современное линейное программирование*, Мир, М., 1984, 224с.

[OA] *Общая алгебра: группы, кольца и модули*, Наука, М., 1990, 590с.

[Pa] Б. Парлетт, *Симметричная проблема собственных значений. Численные методы*, Мир, М., 1983, 382с.

[Pi] С. Писсанецки, *Технология разреженных матриц*, Мир, М., 1988, 411с.

[Po] М. М. Постников, *Линейная алгебра и дифференциальная геометрия*, Наука, М., 1979, 336с.

[Pr] В. В. Прасолов, *Задачи и теоремы линейной алгебры*, Наука, М., 1996, 302с.

[Pro] И. В. Проскуряков, *Сборник задач по линейной алгебре*, Наука, М., 1978, 384с.

[Ra] Д. А. Райков, *Векторные пространства*, Физматгиз, М., 1962.

[Ro] Р. Рокафеллар, *Выпуклый анализ*, Мир, М., 1973, 469с.

[Sk] Л. А. Скорняков, *Элементы алгебры*, Наука, М., 1981, 243с.

[St] Г. Стренг, *Линейная алгебра и ее применения*, Мир, М., 1980, 454с.

[Tu] Р. Тьюарсон, *Разреженные матрицы*, Мир, М., 1977.

[Wi] Дж. Х. Уилкинсон, *Алгебраическая проблема собственных значений*, Наука, М., 1970.

[F] Д. К. Фаддеев, *Лекции по алгебре*, Наука, М., 1984, 416с.

[FS] Д. К. Фаддеев, И. Я. Соминский, *Сборник задач по высшей алгебре*, Наука, М..

[FF] Д. К. Фаддеев, В. Н. Фаддеева, *Вычислительные методы линейной алгебры*, Физматгиз, М., 1960, 656с.

[Fa] К. Фейс, *Алгебра: кольца, модули, категории.* Т. 1, 1977, 676с.

[FM] Дж. Форсайт, К. Молер, *Численное решение систем линейных алгебраических уравнений*, Мир, М., 1969.

[Ha] П. Р. Халмош, *Конечномерные векторные пространства*, РХД, Ижевск, 2002, 263с.

[Hed] Дж. Хедли, *Линейная алгебра для экономистов*, Высшая Школа, М., 1966, 206с.

[HJ] Р. Хорн, Ч. Джонсон, *Матричный анализ*, Мир, М., 1989, 655с.

[Ch] Э. Чезаро, *Элементарный учебник алгебраического анализа и исчисления бесконечно малых. Ч.* I, ОНТИ, Л.–М., 1936, 592с.

[Che] С. Н. Черников, *Линейные неравенства*, Наука, М., 1968, 488с.

[Sha] И. Р. Шафаревич, *Основные понятия алгебры*, R. & C. Dynamics, Ижевск, 1999, 347с.

[Shi] Г. Е. Шилов, *Введение в теорию линейных пространств*, Наука, М., 1956, 304с.

[SchS1] О. Шрайер, Г. Шпернер, *Введение в линейную алгебру в геометрическом изложении*, ОНТИ, М.–Л., 1934, 210с.

[SchS2] О. Шрайер, Г. Шпернер, *Теория матриц*, ОНТИ, М.–Л., 1936, 156с.

ЗАМЫСЕЛ КОНСТРУКТОРА

On the assumption that my technique is either complicated or original or both, the publishers have politely requested me to write an introduction to this book.
At least my theory of technique, if I have one, is very far from original; nor is it complicated. I can express it in fifteen words by quoting The Eternal Question And Immortal Answer of burlesk, viz. "Would you hit a woman with a child? — No, I'd hit her with a brick."[5] Like that burlesk comedian I am abnormally fond of that `movement` which creates `precision`.

e. e. cummings, *is 5*[6]

Se rappeler qu'un tableau — avant d'être un cheval de bataille, une femme nue ou une quelconque anecdote, — est essentielement une surface plane recouverte de couleurs en un certain ordre assemblées. — Никогда не забывайте, что — прежде, чем стать боевой лошадью, обнаженной женщиной или посредственным анекдотом, — картина в сущности представляет собой `плоскую поверхность`, покрытую красками в определенном порядке.

Maurice Denis, *Théories*

1. Архитектоника: горизонтальное членение. Выбор материала в настоящей книге и многие ее композиционные особенности определяются следующим обстоятельством. Она представляет собой **четвертую** часть **`тетралогии`**, части которой срифмованы по схеме ABBA:

Книга I. Не совсем наивная теория множеств

Книга II. Конкретная теория групп

Книга III. Конкретная теория колец

Книга IV. Не совсем наивная линейная алгебра

В то же время — как и в лекциях — я предпринимал все возможные усилия, чтобы минимизировать зависимость частей друг от друга. Большинство определений, многие формулировки и даже некоторые короткие рассуждения повторяются в различных частях. Я не старался быть кратким, я старался быть понятным. Естественно, в пределах отведенного времени. Как уже многократно отмечалось, главным недостатком этой книги является то, что она слишком коротка.

---

[5] Во французском переводе этот диалог передан так: "J'ai trois enfants sur les bras — Mets-les à terre." — "У меня на руках трое детей. — Поставь их на землю."

[6] Воспроизводится `as is`. Орфография и пунктуация сохраняют все странности американского оригинала.

2. Кому и зачем. Курс рассчитан, в первую очередь, на следующие категории читателей:

• Как **современный базовый учебник** для всех, кто впервые *серьезно* знакомится с алгеброй, скажем на младших курсах университета, в рамках таких специальностей, как прикладная математика, программирование, математическая экономика, теоретическая физика, квантовая химия, теория управления, кристаллография, криптография и кодирование.

• Как **вспомогательный элементарный учебник** для студентов первого курса в области чистой математики. Однако, с точки зрения профессионального математика этот учебник в целом слишком консервативен и аналитически ориентирован. Для математика его чтение должно сопровождаться изучением более продвинутых источников, подчеркивающих теоретико-категорные, топологические и геометрические аспекты рассматриваемых понятий.

• Как **дополнительный задачник** средне высокого уровня. Однако, я не пытаюсь конкурировать с стандартными задачниками и привожу очень мало рутинных однотипных задач. Кроме того, многие задачи жестко привязаны к месту их появления и не могут быть решены начинающим сами по себе, в отрыве от антуража.

• Как **справочник** для математиков-неспециалистов, ученых — физиков, химиков и кристаллографов, инженеров, экономистов и в первую очередь специалистов по теории кодирования, теории информации и теории управления, программистов, — словом тех, кто в принципе уже когда-то что-то слышал об алгебре, но забыл слова `идеал` и `гомоморфизм`, хочет освежить свои знания или быстро получить справку по конкретному вопросу.

• Как **Schatzgrube** (=`treasure-trove`) для всех, кто преподает алгебру на университетском уровне и продумывает различные возможности построения курса, или просто ищет новые примеры и вычисления, новые образы, новые задачи или более простые доказательства основных фактов.

• Как **книгу для чтения** дли широких кругов образованных читателей обладающих некоторым досугом: "пенсионеров, школьников старших классов и способных аспирантов"[7].

• Как **памятник русской словесности** для Василеостровских автохтонов и приравненных к ним, для тех, кто интересуется доктринальными, мистическими, психологическими и историческими аспектами математики, для всех, кто увлекается духовной жизнью, мифологией и культурой Санкт-Петербурга, и вообще для всех, кто может, умеет и хочет читать по-русски.

3. Архитектоника: вертикальное членение. В соответствии с этим изложение `эксплицитно` разделено на **пять** МАРКИРОВАННЫХ *четко различающихся* уровней:

[7]Сан Саныч Кириллов, предисловие к изданию 1972 года "Теория представлений", стр. 5, из последующих изданий эта блистательная `локуция` исключена.

- для инженеров $\diamondsuit$,
- для физиков $\heartsuit$,
- для математиков $\spadesuit$,
- для алгебраистов $\clubsuit$,
- для любознательных школьников и пенсионеров ✠

Маркировка первых четырех уровней отвечает рангам мастей в скате. Начинающий должен иметь в виду, что внутри любого параграфа ему могут встретиться фрагменты или комментарии профессионального и/или любительского уровня, которые никак отдельно не выделяются! Если при первом чтении ей непонятно что-то напечатанное мелким шрифтом, это нормально, нужно просто ДВИГАТЬСЯ ДАЛЬШЕ, понимание придет: THE FOCUS IS ON GOING FORWARD, BECAUSE MATHEMATICS IS *only* LEARNED IN HINDSIGHT.

Вопросы, маркированные $\diamondsuit$ и $\heartsuit$, обычно входят в общие курсы алгебры, читаемые в СПбГУ прикладным математикам, при этом ВОПРОСЫ С МЕТКОЙ $\diamondsuit$ РАССКАЗЫВАЮТСЯ ДЕТАЛЬНО И ИХ ЗНАНИЕ НЕОБХОДИМО ДЛЯ ПОЛУЧЕНИЯ УДОВЛЕТВОРИТЕЛЬНОЙ ОЦЕНКИ, в то время как вопросы с меткой $\heartsuit$ часто освещаются менее подробно или только упоминаются. Студенты по отделению чистой математики, которым читается более продвинутый курс алгебры, должны *полностью* владеть уровнем $\heartsuit$ и большинством тем с меткой $\spadesuit$, хотя точный список может от года к году слегка меняться. Наконец, темы с меткой $\clubsuit$ обычно включаются *только* в специальные курсы для студентов, специализирующихся по кафедре алгебры и теории чисел.

В действительности различие между $\diamondsuit$ и $\heartsuit$ не столько в уровне сложности, сколько в уровне императивности. Некоторые темы маркированы $\heartsuit$ не потому, что они труднее или менее важны, а только потому, что они меньше связаны с другими темами в этом курсе или других курсах, читаемых на математико-механическом факультете. То же самое относится к $\spadesuit$ и $\clubsuit$, но, конечно, между $\diamondsuit$ и $\heartsuit$ с одной стороны и $\spadesuit$ и $\clubsuit$ с другой, в целом происходит **зримый** рост требований к зрелости, мотивации и/или настойчивости потенциального читателя.

4. Невский диалект. Настоящий учебник написан на русском языке, *как я его понимаю*. Кроме нормативного великорусского языка знающий глаз и тренированное ухо легко зарегистрируют в моем дискурсе пласты петербургского койне, шихты василеостровского вернакуляра, формации математического арго, страты университетской кафаревусы и спорадические интарсии германо-паданского идиолекта.

Я родился и учился *между выцветших линий* Васильевского острова и язык, которым я говорю, — это городской язык, **Невский диалект**. На диалекте написано *почти* все, что известно как Русская литература. Будучи *фактической* записью моих лекций, эта книга сохраняет большую часть особенностей Василеостровской *разговорной* речи — в том числе непринужденную инкорпорацию фрагментов на основных европейских языках: el estilo que tengo me es natural y sin afectación ninguna: escribo come hablo*, wir loben uns wohl den, der so schreibt, daß man ihn sprechen hört, nicht aber den, der so spricht, daß man ihn schreiben sieht*. Разумеется, мой текст *значительно* беднее, чем разговорная речь: от систематического использования китайских, японских, санскритских, арабских, персидских, ивритских слов и речений по типографским и прагматическим причинам пришлось отказаться.

5. Рекомендации по чтению. Новичку, чтобы начать ориентироваться в предмете и увидеть хотя бы часть внутренних связей, нужно прочесть книгу *дважды*.

• Первый раз так:

○ прочесть все параграфы всех глав, помеченные ♢,

○ вернуться к началу и прочесть все параграфы всех глав, помеченные ♡,

○ вернуться к началу и прочесть все параграфы всех глав, помеченные ♠.

• Второй раз — не менее, чем через 3–4 месяца, лучше через 6–8 месяцев после первого чтения, когда многие детали уже забылись, но общее впечатление еще осталось — можно читать подряд, включая формулировки, но пропуская доказательства в параграфах, помеченных ♣.

Вообще, начинающий должен иметь в виду, что ОПРЕДЕЛЕНИЯ, ПРИМЕРЫ, КОНСТРУКЦИИ И МЕТОДЫ ВАЖНЕЕ, ЧЕМ ПОДАВЛЯЮЩЕЕ БОЛЬШИНСТВО ДОКАЗАТЕЛЬСТВ И ФОРМУЛИРОВОК. Доказательства нужны главным образом для того, чтобы выяснить новые детали и проверить, правильно ли Вы понимаете смысл и пафос того, что говорится.

• Однако сам я предпочитаю читать книги с *произвольного* места, обращаясь к предшествующему по мере необходимости. Эта книга задумана и СКОМПОНИРОВАНА[8] именно для такого чтения, чему должны способствовать детальное оглавление, подробные указатели, большое количество **`реприз`**, **`трассировок`**, **`реитераций`**, **`тавтегорий`** и внутренних ссылок.

6. Copyleft notice. ВСЕ МЫСЛИ, КОТОРЫЕ МОГУТ ПРИЙТИ В ГОЛОВУ ПРИ ЧТЕНИИ ДАННОЙ КНИГИ, ЯВЛЯЮТСЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТЬЮ АВТОРА И ОБЪЕКТОМ АВТОРСКОГО ПРАВА. ИХ НЕЛИЦЕНЗИРОВАННОЕ ОБДУМЫВАНИЕ ЗАПРЕЩАЕТСЯ[9].

---

*МОЙ СТИЛЬ ДЛЯ МЕНЯ НАТУРАЛЕН И ЛИШЕН КАКОЙ-ЛИБО АФФЕКТАЦИИ: Я ПИШУ ТОЧНО ТАК ЖЕ, КАК ГОВОРЮ.

*МЫ ПРИВЕТСТВУЕМ ТОГО, КТО ПИШЕТ ТАК, ЧТО СЛЫШНО, КАК ОН ГОВОРИТ, А ВОВСЕ НЕ ТОГО, КТО ГОВОРИТ ТАК, ЧТО ВИДНО, КАК ОН ПИШЕТ.

[8] Я КОМПОНИРОВАЛ **`Тристана`** ПОД ВЛИЯНИЕМ БОЛЬШОГО ЧУВСТВА И ПОСЛЕ ТРЕХ ЛЕТ ТЕОРЕТИЧЕСКОЙ РАБОТЫ — Рихард Вагнер.

[9] Виктор Пелевин, Generation “П”.

Глава 1. МОДУЛИ

— Вот был у нас офицер, его сиятельство граф Толстой, вот уже матерщинник был, слова просто не скажет, так загибает, что и не выговоришь.

Андрей Николаевич Крылов. *Мои воспоминания*

Основными объектами линейной алгебры — в ее классическом понимании — являются модули и линейные отображения.

Модуль — это абелева группа с операторами. Иными словами, элементы модуля $u, v, \dots$, обычно называемые **векторами**, можно складывать между собой и умножать на некоторые другие объекты $\alpha, \beta, \dots$, называемые **операторами** — а во многих реально возникающих случаях, **скалярами**. Эти операции позволяют определить **линейную комбинацию** векторов $u\alpha + v\beta$. При этом операторы должны сами образовывать кольцо, а определяющие модуль операции — обладать обычными свойствами.

В качестве отображений между модулями естественно рассматривать **линейные отображения**, являющиеся операторами, действующими с противоположной к исходным операторами стороны, и переводящие линейную комбинацию векторов в *такую же* линейную комбинацию их образов: $\phi(u\alpha + v\beta) = \phi(u)\alpha + \phi(v)\beta$.

Оказывается, такие структуры и отображения встречается в математике *чрезвычайно* часто. Фактически *любые* объекты, которые можно разумным образом складывать — числа, многочлены, последовательности, матрицы, функции, линейные операторы, векторные и тензорные поля, дифференциальные формы, меры, ростки функций, etc., etc., etc. — образуют модули над подходящими кольцами.

Важнейшими частными случаями модулей являются **векторные пространства** = модули над полями и **абелевы группы** = модули над кольцом целых чисел. Но в действительности все возникающие в приложениях за пределами алгебры и комбинаторики векторные пространства естественно рассматривать не просто как векторные пространства с умножением на вещественные или комплексные числа, а как модули над различными кольцами функций или дифференциальных операторов.

Точно также, многие естественно возникающие в математике и ее приложениях функции, отображения, операторы, преобразования, etc. являются в действительности линейными отображениями. Например, линейно умножение на фиксированный элемент в любом кольце, или умножение на матрицу, линейны все обычно рассматриваемые в анализе операции такие, как переход к пределу, дифференцирование, интегрирование, etc., etc., etc. Как мы проиллюстрируем в главе 4, громадную часть классического анализа и опирающихся на него дисциплин можно истолковать как приложения или иллюстрации линейной алгебры.

§ 1$\diamondsuit$. Модули и векторные пространства

> "Look here! Wot is the good of having two clocks if they are both different times?"
> "And what", said the porter, "would be the good of having two clocks, if they were both the same time."
>
> Lord Dunsany, *My Ireland*

Пусть вначале R — ассоциативное, но не обязательно коммутативное кольцо с 1.

1. Модули. Следующее определение вводит одну из **важнейших** алгебраических структур, обобщающих **одновременно** понятия абелевой группы, векторного пространства и идеала. Собственно, сам термин `модуль` = `Modul`, `module`[10] как раз и обязан своим происхождением специальному случаю идеалов колец и исторически возник из выражения `сравнение по модулю`.

Определение. *Аддитивно записываемая абелева группа M называется* **левым модулем над** R (*коротко,* **левым** R**-модулем**), *если элементы R действуют на M в качестве* **левых операторов**, *т.е. задано отображение*

$$R \times M \longrightarrow M, \qquad (\lambda, x) \mapsto \lambda x,$$

— умножение элементов M на элементы R слева — причем выполняются следующие четыре аксиомы.

V1 Внешняя ассоциативность:

$$(\lambda\mu)x = \lambda(\mu x)$$

для любых $\lambda, \mu \in R$, $x \in M$.

V2 Дистрибутивность относительно сложения скаляров:

$$(\lambda + \mu)x = \lambda x + \mu x$$

для любых $\lambda, \mu \in R$, $x \in M$.

V3 Дистрибутивность относительно сложения элементов модуля:

$$\lambda(x + y) = \lambda x + \lambda y$$

для любых $\lambda \in R$, $x, y \in M$.

---

[10] Как всегда, русское чтение воспроизводит немецкое. Мне не доводилось встречать ни одного русского математика, который мог бы с первого раза не то, что произнести, а просто *понять* слово `маджул` по-английски.

V4 унитальность:

$$1x = x \qquad \text{для любого } x \in M.$$

Аналогично определяются **правые R-модули**. *При этом элементы R должны действовать в качестве* **правых операторов**,

$$M \times R \longrightarrow M, \qquad (x, \lambda) \mapsto x\lambda,$$

так что аксиома V1 *должна быть заменена на следующую аксиому:*

V1° Внешняя ассоциативность:

$$x(\lambda\mu) = (x\lambda)\mu.$$

для любых $\lambda, \mu \in R$, $x \in M$.

Когда кольцо R фиксировано, оно часто называется **основным кольцом** = Grundring, ground ring. Впрочем, некоторые устойчивые выражения, такие как смена базы, подразумевают романский вариант этого термина: anneau de base, anello di base. Если основное кольцо определено из контекста, о модулях над ним часто говорят просто о как о левых/правых модулях. В случае, когда кольцо R коммутативно, оно называется также **кольцом скаляров** = Skalarenring, scalar ring. Изредка мы будем ссылаться на элементы R как **скаляры** и в том случае, когда R некоммутативно, но строго говоря, это злоупотребление.

Обратите внимание на различие аксиом V1 и V1°: в первом случае x вначале умножается на второй из действующих скаляров, а во втором — на первый. Особенно важен случай, когда кольцо R коммутативно. В этом случае порядок скаляров не важен и, следовательно, аксиомы V1 и V1° эквивалентны, так что любой левый R-модуль можно превратить в правый и наоборот, полагая $x\lambda = \lambda x$. В этом случае говорят просто о **модулях над** R или об **R-модулях**.

В общем случае левый R-модуль можно трактовать как правый R^o-модуль, где R^o — кольцо, противоположное к R. А именно, пусть $^o : R \longrightarrow R^o$, $\lambda \mapsto \lambda^o$, есть канонический антиавтоморфизм колец R и R^o. Тогда полагая $x\lambda^o = \lambda x$ мы превращаем левый R-модуль в правый R^o-модуль. Точно так же правый R-модуль превращается в левый R^o-модуль. Это значит, что мы могли бы рассматривать *только* левые или *только* правые модули. Это, однако, было бы неудобно, так как во многих конструкциях естественно *одновременно* рассматривать как левые, так и правые модули. Кроме того, очень часто возникают объекты, которые одновременно являются левым модулем над одним кольцом и правым модулем над другим.

В некоммутативном же случае указание на то, левые или правые модули рассматриваются, *обязательно*. Чтобы указать, что M рассматривается как *левый* модуль, часто пишут $_RM$, а *правый* — M_R. Наиболее ригорозные авторы резервируют термин **R-модуль** исключительно для *левых* модулей над R, при этом *правый* модуль над R называется **модуль-R**.

Определение. *В случае, когда $R = T$ является телом, вместо левых и правых модулей над T говорят о* **левых** *или правых векторных пространствах над T. В случае, когда $R = K$ — поле, говорят просто о* **векторных пространствах** *над K. Элементы векторного пространства часто называются* **векторами**, *в противоположность элементам тела T, которые называются* **скалярами**.

Предостережение. Многие писатели в области анализа, дифференциальных уравнений и т.д. называют *бесконечномерные* векторные пространства **линейными пространствами**. Мы не различаем термины `векторное пространство` и `линейное пространство` и используем их как синонимы, независимо от того, конечномерны они или нет.

Предостережение. Полезно понимать, что тот факт, что операция в V записывается аддитивно, является чистой условностью. Например, $\mathbb{Q}^*$ с операцией умножения как сложением и возведением в целую степень как умножением на скаляры удовлетворяет всем аксиомам (правого) модуля:

$$\mathbf{V1}^\circ\ x^{mn} = (x^m)^n; \qquad \mathbf{V2}\ x^{m+n} = x^m x^n;$$

$$\mathbf{V3}\ (xy)^n = x^n y^n; \qquad \mathbf{V4}\ x^1 = x.$$

Сформулируем несколько простейших следствий из аксиом модуля.

Задача. Докажите, что для любых $\forall \lambda, \mu \in R$, $\forall x, y \in M$, выполняются тождества

- $0x = 0$;
- $\lambda 0 = 0$;
- $(-\lambda)x = -\lambda x = \lambda(-x)$;
- $(\lambda - \mu)x = \lambda x - \mu x$;
- $\lambda(x - y) = \lambda x - \lambda y$.

Задача (`allgemeine Distributivgesetz`). Докажите, что в любом модуле выполняется **обобщенная дистрибутивность** умножения на скаляры относительно сложения:

$$(\alpha_1 + \ldots + \alpha_m)(x_1 + \ldots + x_n) = \sum_{i,j} \alpha_i x_j.$$

2. Бимодули. Предположим, что на M *одновременно* заданы структуры левого R-модуля и правого S-модуля. Говорят, что эти структуры *согласованы*, если выполняется следующая аксиома, утверждающая, что скаляры из R и S коммутируют. Заметим, что эта аксиома аналогична аксиоме, связывающей два умножения в алгебре.

V5 $\forall \lambda \in R, \forall x \in M, \forall \mu \in S, (\lambda x)\mu = \lambda(x\mu)$ (внешняя ассоциативность).

В этом случае M называется **бимодулем** или, если чтобы подчеркнуть, что M рассматривается как бимодуль, пишут ${}_R M_S$ и говорят об M как об R-**модуле**-S или иногда как об R-**бимодуле**-S.

Можно было бы рассматривать два левых или два правых действия и писать ${}_{R,S}M$ или $M_{R,S}$. Это подразумевает, что операторы из R и S коммутируют, т.е., например, в случае левого действия

$$(\lambda\mu)x = \lambda(\mu x), \qquad \lambda \in R,\ \mu \in S,\ x \in M.$$

Модуль M, на котором заданы коммутирующие левые действия колец R и S, называется (R, S)-**бимодулем**. Правые (R, S)-**бимодули** — или коротко **бимодули**-(R, S) — определяются аналогично. Однако на практике *гораздо* чаще встречается случай, когда два кольца действуют на M с *разных* сторон.

Комментарий. С использованием понятия тензорного произведения алгебр изучение бимодулей сводится к изучению обычных модулей над другим кольцом. Например, R-модуль-S можно M рассматривать как *левый* (R, S^o)-бимодуль, а его, в свою очередь — как левый модуль над $R \otimes S^o$. С другой стороны, тот же модуль можно рассматривать как *правый* (R^o, S) бимодуль или, что то же самое, как правый модуль над $R^o \otimes S$.

§ 2♢. Примеры модулей

I'll show you a thing or three.

Groucho Marx

В настоящем параграфе мы ограничимся перечислением нескольких первых примеров R-модулей и векторных пространств. Много дальнейших более рафинированных или более специальных примеров встретится нам в дальнейшем.

• **Нулевой модуль.** Множество $\{0\}$, состоящее из одного элемента 0, вместе с операциями $0 + 0 = 0$, $\lambda 0 = 0$ для всех $\lambda \in R$, является R-модулем. Этот модуль называется **нулевым модулем** и обычно обозначается просто 0.

• **Эвклидовы пространства.** Обычные векторы на эвклидовой плоскости $\mathbb{R}^2$ и в трехмерном эвклидовом пространстве $\mathbb{R}^3$ образуют векторные пространства над $\mathbb{R}$. Этот пример был впервые явно рассмотрен Симоном Стевином в конце XVI века.

• **Абелевы группы.** Любая абелева группа M является модулем над $\mathbb{Z}$, если положить для $n \in \mathbb{N}$ и $x \in M$:

$$nx = x + \ldots + x \ \ (n \text{ раз}), \qquad 0x = 0, \qquad (-n)x = n(-x).$$

• **Абелевы группы (cont.)** Любая абелева группа M является левым модулем над $\mathrm{End}(M)$. В самом деле, V1, V2 и V4 — это просто определение операций в $\mathrm{End}(M)$, а V3 — это определение эндоморфизма.

• **Дифференциальные абелевы группы.** Пусть $R = \mathbb{Z}[d]$, где $d^2 = 0$ — кольцо двойных чисел над $\mathbb{Z}$. Тогда R-модуль — это в точности абелева группа M, в которой зафиксировано **дифференцирование** $a \mapsto da$, т.е. такой эндоморфизм, квадрат которого равен 0.

• **Кольцо как модуль над собой.** Само кольцо R можно рассматривать как левый и как правый R-модуль. А именно, пусть $M = {}_RR$ совпадает с R как аддитивная группа, а левое умножение на элементы R задается формулой $x \mapsto \lambda x$, где $\lambda \in R$, $x \in M$. Тогда из аксиом кольца вытекает, что ${}_RR$ — левый R-модуль. Аналогично, полагая, что $M = R_R$ совпадает с R как аддитивная группа, а правое умножение на элементы R задается формулой $x \mapsto x\lambda$, где $x \in M$, $\lambda \in R$, мы задаем на R структуру правого R-модуля. Получающийся модуль называется обычно **левым/правым свободным R-модулем ранга 1**.

• **Идеалы.** Каждый левый идеал I кольца R является левым R-модулем, правый идеал I — правым R-модулем, а двусторонний идеал I — бимодулем, или, если нужна особая точность, R-модулем-R.

• **Идеализация модуля.** В действительности, каждый R-модуль-R можно естественно рассматривать как идеал в некотором кольце. А именно, введем на прямой сумме $R \oplus V$ абелевых групп R и V следующее умножение

$$(\alpha, u)(\beta, v) = (\alpha\beta, \alpha v + u\beta).$$

Легко проверить, что это умножение превращает $R \oplus V$ в ассоциативное кольцо, причем V идеал в $R \oplus V$, квадрат которого равен 0. Таким образом, в коммутативном случае КАЖДЫЙ МОДУЛЬ МОЖЕТ РАССМАТРИВАТЬСЯ КАК ИДЕАЛ НЕКОТОРОГО КОЛЬЦА.

• **Дробные идеалы.** Пусть R — область целостности, K ее поле частных. Ненулевой подмодуль $I \leq K$ называется дробным идеалом кольца R, если существует такое $\lambda \in R^\bullet$, что $\lambda I \leq R$. Каждый ненулевой идеал R кольца является дробным идеалом.

Следующий *важнейший* пример модулей будет подробно рассмотрен в следующем параграфе.

• **Свободные модули.** Обозначим через ${}^nR$ — множество всех **строк длины** n а через R^n — множество всех **столбцов высоты** n с компонентами из R. Тогда ${}^nR$ является *левым*, а R^n — *правым* модулем над R. Они называются, соответственно, **свободным левым** и **свободным правым модулями** над R **ранга** n.

• В дополнение к предыдущему примеру необходимо упомянуть, что ${}^nR$ является *правым*, а R^n — *левым* модулем над кольцом матриц $M(n, R)$, относительно обычного умножения столбца на матрицу слева и строки на матрицу справа.

• Кольцо многочленов $R[x]$ от переменной x над кольцом R можно рассматривать как R-модуль относительно обычной операции сложения многочленов и операции умножения многочлена на константу.

• Множество $M(m, n, R)$ матриц размера $m \times n$ с коэффициентами из кольца R можно рассматривать R-модуль-R относительно обычного сложения матриц и умножения матриц на скаляры слева и справа.

• В действительности множество $M(m,n,R)$ имеет естественную структуру $M(m,R)$-модуля-$M(n,R)$ относительно обычного умножения матриц размера $m\times n$ на квадратные матрицы степени m слева и на квадратные матрицы степени n справа.

• Если L/K — расширение полей, т.е. $K\subseteq L$, то L можно рассматривать как векторное пространство над K. Например, $\mathbb{C}$ - векторное пространство над $\mathbb{R}$, $\mathbb{R}$ — векторное пространство над $\mathbb{Q}$, а $\mathbb{F}_4$ — векторное пространство над $\mathbb{F}_2$.

• **Пространство функций.** Множество $K^X=\mathrm{Map}(X,K)$ всех функций на некотором множестве X со значениями в поле K является векторным пространством над K относительно обычного (поточечного) сложения функций и (поточечной) операции умножения функции на константу:

$$(f+g)(x)=f(x)+g(x),\qquad (\lambda f)(x)=\lambda f(x).$$

В дальнейшем всегда, когда мы говорим о пространствах функций, мы имеем в виду какие-то подпространства K^X замкнутые относительно этих операций.

• **Модули над групповым кольцом.** Пусть K — поле, G — конечная группа, а $K[G]$ — групповое кольцо группы G над K. Линейным представлением группы G степени n над полем K называется гомоморфизм $\rho: G\longrightarrow \mathrm{GL}(V)$, в полную линейную группу n-мерного векторного пространства V над K. Полагая $gv=\rho(g)v$ и продолжая это действие по линейности на все кольцо $K[G]$, мы задаем на V структуру левого $K[G]$-модуля.

§ 3$\diamondsuit$. Свободные модули

В элементарной линейной алгебре обычно ограничиваются рассмотрением свободных модулей, т.е. модулей, в которых существует базис. Это понятие детально обсуждается вследующей главе, но уже сейчас удобно привести два основных примера. В действительности, *с точностью до изоморфизма* никаких других конечно порожденных свободных модулей нет.

• **Свободный левый модуль.** Следуя Кону обозначим через ${}^nR$ множество всех **строк длины** n с компонентами из R, рассматриваемое как левый R-модуль. Иными словами, элементами ${}^nR$ являются все строки вида

$$x=(x_1,\dots,x_n),\qquad x_i\in R,$$

причем операции вводятся покомпонентно:

$$(x_1,\dots,x_n)+(y_1,\dots,y_n)=(x_1+y_1,\dots,x_n+y_n),$$

$$\lambda(x_1,\dots,x_n)=(\lambda x_1,\dots,\lambda x_n).$$

Получающийся модуль называется **свободным левым R-модулем ранга** n. Вообще, свободным левым R-модулем ранга n называется любой модуль V, изоморфный ${}^nR$, его ранг обозначается $n = \mathrm{rk}(V)$.

• **Свободный правый модуль.** Как обычно, R^n обозначает множество всех **столбцов высоты** n с компонентами из R, рассматриваемое как правый R-модуль. Иными словами, элементами R^n являются все столбцы вида

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \qquad x_i \in R,$$

а операции сложения и умножения на множестве столбцов вводятся покомпонентно:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}, \qquad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \lambda = \begin{pmatrix} x_1\lambda \\ \vdots \\ x_n\lambda \end{pmatrix}$$

Получающийся модуль называется **свободным правым R-модулем ранга** n. Вообще, свободным правым R-модулем ранга n называется любой модуль V, изоморфный R^n, его ранг обозначается $n = \mathrm{rk}(V)$.

Предостережение 1. Для экономии места мы часто записываем столбец x в виде $x = (x_1, \ldots, x_n)^T$, как результат применения операции **формального транспонирования** к строке $(x_1, \ldots, x_n)$. Следует, однако, иметь в виду, что эта операция совпадает с настоящей операцией транспонирования матриц **только** в случае, когда кольцо R коммутативно. В этом последнем случае модули R^n и ${}^nR$ будут изоморфны как R-модули, и называются **свободным R-модулем ранга** n. Тем не менее, **даже** в случае коммутативного основного кольца их необходимо **тщательно различать**. На поверхностном уровне это будет очевидно сразу, как только мы определим матрицы. В дальнейшем вскроются гораздо более глубокие причины. Дело в том, что ${}^nR$ является правым $M(n, R)$-модулем, а R^n — левым $M(n, R)$-модулем. Иными словами, это значит, что R-изоморфизм между ${}^nR$ и R^n, задаваемый транспонированием, не является каноническим, а связан с конкретным выбором базисов. Задание конкретного изоморфизма между ${}^nR$ и R^n вводит на R^n дополнительную структуру.

Предостережение 2. Подмодуль свободного модуля не обязан быть свободным. Например, если $x \in R$ — делитель нуля, то идеал $Rx \leq R$ не является свободным R-модулем. Более того, вообще говоря даже прямое слагаемое свободного модуля не обязано быть свободным. Прямые слагаемые свободных модулей называются **проективными** модулями. Вопрос о том, для каких классов колец R все проективные модули над R свободны, представляет собой один из центральных вопросов одного из центрального разделов алгебры — **алгебраической K-теории**.

• **Прямая сумма.** Оба эти примера являются частными случаями конструкции прямой суммы модулей. А именно, пусть $M_1, \ldots, M_n$ суть левые R-модули. Определим левый Λ-модуль $M = M_1 \oplus \ldots \oplus M_n$, считая, что как множество M совпадает с прямым произведением $M_1 \times \ldots \times M_n$, т.е., иными словами, состоит из всех n-к $(x_1, \ldots, x_n)$, где $x_i \in M_i$, а операции сложения и умножения на скаляр в M вводятся покомпонентно, т.е.

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),$$

$$\lambda(x_1, \dots, x_n) = (\lambda x_1, \dots, \lambda x_n).$$

Эти операции действительно превращают M в левый R-модуль, называемый прямой суммой левых R-модулей $M_1, \dots, M_n$. Прямая сумма правых R-модулей определяется аналогично и сама является правым R-модулем. При этом ${}^nR = {}_RR \oplus \dots \oplus {}_RR$ и $R^n = R_R \oplus \dots \oplus R_R$ (в каждом из этих прямых разложений n слагаемых).

• **Кольца свободных идеалов.** Кольцо R называется **кольцом свободных левых идеалов**, если все его левые идеалы являются свободными левыми R-модулями. **Кольцо свободных правых идеалов** определяется аналогично.

Задача. Докажите, что коммутативное кольцо в том и только том случае является кольцом свободных идеалов, когда оно кольцо главных идеалов.

В некоммутативном случае аналогичное утверждение безнадежно неверно и имеется множество нетривиальных примеров и обширная теория, посвященная кольцам свободных идеалов, см., например, [Co].

§ 4♢. Линейные отображения

Люди, заключающие договор с дьяволом, колдуны и чернокнижники родятся левшами.

Дмитрий Сергеевич Мережковский. *Воскресшие боги*

Сейчас мы введем класс отображений, согласованных со структурой модуля/векторного пространства.

Определение. *Пусть U и V — два правых R-модуля. Отображение $f : U \longrightarrow V$, $u \mapsto f(u)$, называется* **гомоморфизмом** *R-модулей, (или просто* **морфизмом** *R-модулей), если оно удовлетворяет следующим двум условиям.*

H1 Аддитивность:

$$f(x + y) = f(x) + f(y)$$

для любых $x, y \in U$,

H2 Однородность степени 1:

$$f(x\lambda) = f(x)\lambda$$

для любых $\lambda \in R$, $x \in U$.

Вместе два эти условия часто называются также **линейностью** или, точнее, **R-линейностью**. Совместно они означают, что каждая линейная комбинация векторов переходит под лействие f в линейную комбинацию образов *с теми же коэффициентами*:

$$f(u\alpha + v\beta) = f(u)\alpha + f(v)\beta.$$

Совершенно аналогично определяются и морфизмы левых R-модулей, при этом в большинстве элементарных учебников аксиома (H2) переписывается в виде

H2′ Однородность степени 1:

$$f(\lambda x) = f(\lambda x),$$

для любых $\lambda \in R$, $x \in M$.

Однако специалисты в области теории колец знают, что даже в случае, когда кольцо R коммутативно, гомоморфизмы левых модулей можно записывать *только* справа. Отображение $f : M \longrightarrow N$, $u \mapsto (u)f$, левых модулей называется гомоморфизмом левых R-модулей, если

$$(x + y)f = (x)f + (y)f, \qquad (\lambda x)f = \lambda(x)f,$$

для любых $x, y \in U$ и любого $\lambda \in R$. Именно в силу непривычности такой записи для большинства читателей в дальнейшем мы предпочитаем работать с правыми, а не с левыми модулями.

Множество всех гомоморфизмов из M в N обозначается через $\mathrm{Hom}(M, N)$ или, если нужно подчеркнуть, что M и N рассматриваются как R-модули, то $\mathrm{Hom}_R(M, N)$.

В частности, можно говорить о гомоморфизмах векторных пространств над полем, в этом случае они обычно называются просто **линейными отображениями** или, если нужно уточнить, о каком именно поле идет речь, **K-линейными отображениями**.

Как обычно, гомоморфизм f называется:

- **мономорфизмом**, если f инъективен;
- **эпиморфизмом**, если f сюръективен;
- **изоморфизмом**, если f биективен;
- **эндоморфизмом**, если $U = V$;
- **автоморфизмом**, если $U = V$, а f биективен.

Таким образом, изоморфизм — это такой гомоморфизм, который является одновременно мономорфизмом и эпиморфизмом; эндоморфизм — это гомоморфизм группы в себя, а автоморфизм – это изоморфизм группы на себя.

Эндоморфизмы векторных пространств обычно называются **линейными операторами**. Множество всех эндоморфизмов R-модуля M обозначается $\mathrm{End}_R(M)$ или просто $\mathrm{End}(M)$. Как мы увидим в дальнейшем, это множество всегда является ассоциативным — но, как правило, некоммутативным! — кольцом с 1, называемым кольцом эндоморфизмов модуля M. В случае векторных пространств говорят обычно о кольце (или алгебре) линейных операторов.

2. Первые примеры. Приведем несколько очевидных примеров линейных отображений.

• Для любых модулей нулевое отображение $0 : M \longrightarrow N$, переводящее все векторы $x \in M$ в 0, является гомоморфизмом M в N.

• Для любого модуля тождественное отображение $\mathrm{id} : M \longrightarrow M$, переводящее каждый $x \in M$ в себя, является эндоморфизмом модуля M.

• Если кольцо R коммутативно, то умножение на любой элемент $\lambda \in R$ задает эндоморфизм модуля M, $x \mapsto x\lambda$, называемый **гомотетией**. В самом деле, линейность вытекает из дистрибутивности умножения вектора на скаляр относительно сложения векторов и коммутативности умножения в кольце R.

• Координатная проекция $\mathrm{pr}_i : R^n \longrightarrow R$, сопоставляющая столбцу его i-ю компоненту, линейна. Вообще, пусть V — какое-то векторное пространство с базисом $e_1, \dots, e_n$. Рассмотрим i-ю **координатную функцию** e_i^*, т. е. отображение, сопоставляющее вектору $x \in V$ его i-ю координату в этом базисе. Из единственности разложения по базису следует, что e_i^* линейно. В самом деле, координаты аддитивны и однородны:

$$e_i^*(u+v) = e_i^*(u) + e_i^*(v), \qquad e_i^*(u)\lambda = e_i^*(u)\lambda.$$

Этот пример будет играть огромное значение в главе, посвященной двойственности.

• Для любой матрицы $x \in M(m,n,R)$ отображение $R^n \longrightarrow R^m$, $u \mapsto xu$, задаваемое умножением на матрицу x *слева*, линейно:

$$x(u+v) = xu + xv, \qquad x(u\lambda) = (xu)\lambda.$$

В действительностьи, в главе, посвященной линейным отображениям, мы узнаем, что никаких других линейных отображений между свободными модулями конечного ранга и не существует. Точно так же каждое линейное отображение ${}^nR \longrightarrow {}^mR$ свободных левых модулей состоит в умножении на некоторую матрицу $y \in M(n,m,R)$ *справа*, т. е. имеет вид $v \mapsto vy$.

• Пусть $K \le L$ — два поля и V — несет согласованные структуры векторного пространства над K и над L. Тогда K-линейное отображение совершенно не обязано быть L-линейным. Пусть, например, $K = \mathbb{R}$, а $L = V = \mathbb{C}$. Тогда комплексное сопряжение, переводящее комплексное число $z = a+bi$ в комплексно сопряженное $\overline{z} = a-bi$, является $\mathbb{R}$-линейным, но не $\mathbb{C}$-линейным, в самом деле, $\overline{iz} = -iz$, а вовсе не iz, как следовало бы из $\mathbb{C}$-линейности.

§ 5♠. Обратная замена кольца

Сейчас мы покажем, что каждый модуль происходит из некоторой абелевой группы A, рассматриваемой как модуль над кольцом $R = \mathrm{End}(A)$. Иными словами, модуль это просто абелева группа с операторами.

1. Обратная замена кольца. Пусть теперь $\phi : R \longrightarrow S$ — гомоморфизм колец с 1. Тогда левый S-модуль M превращается в левый R-модуль, если определить действие R на M следующим образом: $R \times M \longrightarrow M$, $(\lambda, x) \mapsto \lambda * x$, где $\lambda * x = \phi(\lambda)x$. Про построенный так R-модуль говорят, что он получается из S-модуля M **переносом структуры**, (обратной) **заменой базы**, (обратной) **заменой скаляров** или (обратной) **заменой кольца** посредством гомоморфизма ϕ. Чтобы подчеркнуть, что перенос структуры осуществлен именно посредством гомоморфизма ϕ, для построенного так R-модуля иногда используется обозначение ${}_{\phi}M$. Разнобой в терминологии связан с тем, что эти термины представляет собой переводы с разных языков: `base change`, `scalar change`, `Grundringwechsel`, `Ringwechsel` и т.д.

Вот некоторые наиболее важные частные случаи этой конструкции:

• Пусть $R \leq S$ — подкольцо кольца S, а $\iota : R \hookrightarrow S$ — каноническое вложение. Тогда про модуль ${}_{\iota}M$ говорят, что он построен **сужением скаляров**.

• Например, сужая скаляры при помощи гомоморфизма $\iota : \mathbb{Z} \longrightarrow R$, $n \mapsto n1$, мы вообще превращаем R-модуль M в абелеву группу ${}_{\iota}M = M^{+}$.

• Пусть $I \trianglelefteq R$ — идеал кольца R и $\pi : R \longrightarrow R/I$ — каноническая проекция на фактор-кольцо. Если M — некоторый R/I-модуль, то про R-модуль ${}_{\pi}M$ говорят, что он получен **подъемом скаляров** (`Hochhebung von Skalaren`).

• Пусть V — векторное пространство над полем $\mathbb{C}$ комплексных чисел, $\bar{\ } : \mathbb{C} \longrightarrow \mathbb{C}$ — комплексное сопряжение. Пространство $\overline{V}$, совпадающее с V как абелева группа, в котором умножение на скаляр определяется формулой $\lambda * x = \overline{\lambda}x$, называется пространством (комплексно) **сопряженным** с V (не путать с двойственным V^* или сопряженным к двойственному!!!)

• Пусть $R = S = K$ — совершенное поле характеристики $p > 0$, а $F : K \longrightarrow K$, $x \mapsto x^p$ — автоморфизм Фробениуса поля K. Про пространство ${}_{F^{-1}}V$ говорят, что оно является **скручиванием Фробениуса** (`Frobenius twist`) пространства V. Иными словами, как аддитивная группа ${}_{F^{-1}}V$ совпадает с V, но умножение на скаляры задается там следующим образом $\lambda \circ x = \lambda^{1/p}x$.

2. Универсальный пример модуля. Пусть A — произвольная абелева группа, $R = \mathrm{End}(A)$ — кольцо эндоморфизмов A.

Задача. Убедитесь, что A становится $\mathrm{End}(A)$-модулем, если положить $\phi x = \phi(x)$.

Убедимся теперь, что в мифологическом плане это *единственный* пример модуля. Пусть теперь R — произвольное кольцо, а V — произвольный левый R-модуль. Чтобы избежать смешения кольца эндоморфизмов абелевой группы V с рассматриваемым в дальнейшем подкольцом $\mathrm{End}_R(V)$, состоящим из R-эндоморфизмов (обычно, как раз и обозначаемым просто через $\mathrm{End}(V)$), мы будем обозначать кольцо эндоморфизмов V как абелевой группы через $\mathrm{End}_{\mathbb{Z}}(V)$.

Задача. Убедитесь, что для произвольного $\lambda \in R$ гомотетия $\theta_\lambda : V \longrightarrow V$, $x \mapsto \lambda x$ является эндоморфизмом *абелевой группы* V. Проверьте, что сопоставление $\lambda \mapsto \theta_\lambda$ определяет гомоморфизм $R \longrightarrow \mathrm{End}_{\mathbb{Z}}(V)$. Докажите, что каждая структура левого R-модуля на V получается таким образом.

Решение. То, что θ_λ действительно эндоморфизм — это в точности аксиома **V3**. В этих обозначениях аксиому **V3** можно переписать в виде $\theta_{\lambda+\mu} = \theta_\lambda + \theta_\mu$, а аксиому **V1** — в виде $\theta_{\lambda\mu} = \theta_\lambda \theta_\mu$. Наконец, аксиома **V4** означает, что $\theta_1 = \mathrm{id}_V$.

Задача. Установите аналогичное соответствие между структурами *правого* R-модуля на V и *антигомоморфизмами* $R \longrightarrow \mathrm{End}_{\mathbb{Z}}(V)$.

Решение. Единственное отличие от предыдущей задачи состоит в том, что если определить гомотетию $\eta_\lambda : V \longrightarrow V$, $x \mapsto x\lambda$, то аксиома $\mathbf{V1}^\circ$ перепишется в виде $\eta_{\lambda\mu} = \eta_\mu \eta_\lambda$.

Таким образом (по крайней мере, если отображение $R \longrightarrow \mathrm{End}_{\mathbb{Z}}(V)$ инъективно), элементы кольца R естественно рассматривать как **эндоморфизмы** абелевой группы V — или, на традиционном жаргоне, **операторы** действующие на этой группе.

§ 6♣. Прямая замена кольца

Для чуть более софистицированного читателя, который слышал не только о сужении, но и о расширении скаляров, заметим, что кроме обратной замены кольца часто рассматривается **прямая** замена кольца. Однако, так как эта конструкция предполагает знакомство с понятием тензорного произведения, то при первом чтении настоящий пункт следует пропустить. А именно, если $\phi : R \longrightarrow S$ — гомоморфизм колец с 1 и M — некоторый R-модуль, то $M_\phi = S \otimes_R M$ превращается в S-модуль, если положить $\lambda(\mu \otimes x) = \lambda\mu \otimes x$ для любых $\lambda, \mu \in S$ и $x \in M$. Про построенный так S модуль говорят, что он получается (прямой) **заменой базы**, (прямой) **заменой скаляров** или (прямой) **заменой кольца** посредством гомоморфизма ϕ.

Вот некоторые наиболее важные частные случаи этой конструкции:

• Пусть $R \leq S$ — подкольцо кольца S, а $\iota : R \hookrightarrow S$ — каноническое вложение. Тогда про модуль M_ι говорят, что он построен **расширением скаляров**.

• Пусть $I \trianglelefteq R$ — идеал кольца R и $\pi : R \longrightarrow R/I$ — каноническая проекция на фактор-кольцо. Если M — некоторый R-модуль, то про R/I-модуль $M_\pi = M/IM$ говорят, что он получен **редукцией по модулю** I.

• Пусть $S \subseteq R^\bullet$ — мультипликативная система, $\phi_S : R \longrightarrow R_S$ — соответствующий гомоморфизм локализации. Тогда $M_{\phi_S} = M_S = R_S \otimes_R M$ называется **локализацией** модуля M в S или **модулем частных** модуля M относительно мультипликативной системы S.

• Пусть $R = S = K$ — поле характеристики $p > 0$, не обязательно совершенное, а $F : K \longrightarrow K$, $x \mapsto x^p$ — эндоморфизм Фробениуса поля K. Про пространство V_F говорят, что оно является **скручиванием Фробениуса** пространства V. В случае совершенного поля это понятие совпадает с введенным в пункте 1.

Для еще более софистицированного чистателя заметим, что рассмотренная конструкция называется **ковариантной** прямой заменой кольца. Кроме нее рассматривается **контравариантная** прямая замена кольца, при которой R-модулю M сопоставляется S-модуль $M^\phi = \mathrm{Hom}_R(S, M)$. Кроме того, для некоммутативных колец нужно, конечно, следить за тем, идет речь о левых или правых модулях и тщательно различать $S \otimes_R M$ и $M \otimes_R S$.

§ 7♢. Линейные комбинации

Термин “линейная комбинация” на самом деле употребляется в двух смыслах:

∘ как указание действий, которые производятся над данными векторами, что равносильно заданию коэффициентов $\lambda_1, \ldots, \lambda_n$;

∘ как результат этих действий.

В выражении “нетривиальная линейная комбинация данных векторов равна нулю” нетривиальность понимается в первом смысле, а равенство нулю — во втором.

Эрнест Борисович Винберг, [Vi], Гл. 2

Пусть V — правый R-модуль и $v_1, \ldots, v_n \in V$.

Определение. Линейной комбинацией *векторов* $v_1, \ldots, v_n \in V$ *называется*

- *любое* **выражение** *вида* $v_1\lambda_1 + \ldots + v_n\lambda_n$, *где* $\lambda_1, \ldots, \lambda_n \in R$,
- *вектор* $v = v_1\lambda_1 + \ldots + v_n\lambda_n$, *представляемый таким выражением.*

При этом $\lambda_1, \ldots, \lambda_n$ *называются* **коэффициентами** *линейной комбинации.*

Если все коэффициенты $\lambda_1, \ldots, \lambda_n$ равны 0, то линейная комбинация называется **тривиальной**, в противном случае — **нетривиальной**.

Чтобы подчеркнуть, что коэффициенты пишутся *справа*, говорят о **правых линейных комбинациях**. Для элементов левого R-модуля V можно совершенно аналогично определить **левые линейные комбинации** $\lambda_1 v_1 + \ldots + \lambda_n v_n$, в которых коэффициенты пишутся *слева*. Это различие становится по настоящему важным в тех случаях, когда V несет структуру R-бимодуля, например, для некоммутативного кольца R, рассматриваемого как бимодуль над собой. Множество девых линейных комбинаций элемента $x \in R$ совпадает с левым идеалом Rx, порожденным x, в то время как множество его правых линейных комбинаций — это порожденный им правый идеал xR. Ясно, что в общем случае $Rx \neq xR$, так что левые и правые линейные комбинации это совсем не одно и то же.

Понятие линейной комбинации легко обобщается и на случай бесконечного семейства векторов. Если $\{v_\alpha\}$, $\alpha \in \Omega$, — такое семейство, то линейной комбинацией семейства $\{v_\alpha\}$ называется любая сумма вида $\sum v_\alpha \lambda_\alpha$, где $\lambda_\alpha \in K$, причем почти все λ_α равны 0. Иными словами, по опрежедению линейная комбинация бесконечного семейства — это то же самое, что линейная комбинация *какого-то* его конечного подсемейства. Это утверждение обычно называется **принципом компактности** для линейных комбинаций.

Предостережение. Как уже отмечено в эпиграфе, понятие **линейная комбинация** — и, особенно, **коэффициенты линейной комбинации** — заключает *намеренную* двусмысленность. Ситуация, когда в одной фразе один и тот же термин употребляется в двух совершенно различных смыслах типична для физики, но в высшей степени необычна для математики. Поэтому Бурбаки употребляет термин **линейная комбинация** исключительно для обозначения *результата* вычисления линейной комбинации, т.е. получающегося вектора. Однако поскольку эта двусмысленность глубоко укоренилась в литературе по линейной алгебре, мы не пытаемся менять традиционную терминологию и предоставляем читателю каждый раз самостоятельно догадываться, в каком именно смысле употребляется выражение **линейная комбинация**.

Пример. Пусть $V = R^n$ — свободный правый R-модуль ранга n над R. Рассмотрим следующий набор векторов:

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots, \quad e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

где у i-го вектора в i-й позиции стоит 1, а все остальные компоненты равны 0. В дальнейшем набор векторов $e_1, \dots, e_n$ будет называться **стандартным базисом** модуля $V = R^n$. Любой вектор $x \in R^n$ является линейной комбинацией векторов $e_1, \dots, e_n$, а именно,

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = e_1 x_1 + \dots + e_n x_n.$$

§ 8$\diamondsuit$. Подмодули

Введем еще одно ключевое определение.

Определение. *Непустое подмножество U модуля V называется* **подмодулем**, *если оно само является модулем относительно тех же самых операций сложения и умножения на скаляр, что и модуль V, иными словами, если U обладает следующими двумя свойствами.*

S1 Замкнутость относительно сложения:

$$u + v \in U \qquad \text{для любых } u, v \in U.$$

S2 Устойчивость относительно умножения на скаляр:

$$\lambda u \in U \qquad \text{для любых } \lambda \in K,\ u \in U.$$

При этом мы пишем $U \le V$, чтобы обозначить, что U — подмодуль в V, а не просто подмножество. В случае, когда V векторное пространство, U называется **подпространством**.

Эти две аксиомы можно сформулировать и иначе, сказав, что U содержит вместе с двумя любыми своими векторами любую их линейную комбинацию:

$$\lambda u + \mu v \in U \qquad \text{для любых } \lambda, \mu \in K,\ u, v \in U.$$

Тогда, разумеется, то же самое будет выполнено и линейных комбинаций любого числа векторов:

$$\lambda_1 u_1 + \ldots + \lambda_n u_n \in U \qquad \text{для любых } \lambda_1, \ldots, \lambda_n \in K,\ u_1, \ldots, u_n \in U.$$

2. Первые примеры. Приведем несколько очевидных примеров подмодулей.

• Сам модуль V и нулевой подмодуль $0 = \{0\}$, состоящее лишь из нулевого вектора, являются подмодулями в V, называемыми **очевидными**. Подмодуль $U \leq V$ называется **нетривиальным**, если $U \neq 0$ и **собственным**, если $U \neq V$.

• Нетривиальные подпространства эвклидовой плоскости — это прямые, проходящие через 0, а нетривиальные подпространства трехмерного эвклидова пространства — это прямые и плоскости, проходящие через 0.

• Подмодули в левом R-модуле ${}_R R$ — это в точности левые идеалы кольца R, а подмодули в правом R-модуле R_R — это в точности правые идеалы кольца R.

• Пусть $I \trianglelefteq R$ — идеал кольца R, а V — произвольный подмодуль. Множество

$$VI = \{x\lambda \mid x \in V,\ \lambda \in I\}$$

является подмодулем в V.

• Решения линейной однородной системы линейных уравнений образуют подмодуль в R^n. Для поля верно и обратное, никаких других подпространств, кроме пространств решений линейных однородных систем линейных уравнений, в K^n нет.

• Пусть $V = R^X$ — модуль функций на множестве X со значениями в коммутативном кольце R, а $Y \subseteq X$. Положим

$$U = \{f \in V \mid f(y) = 0 \text{ для всех } y \in Y\}.$$

Тогда U является подмодулем в V.

• Пусть $V = R[x]$ — кольцо многочленов, рассматриваемое как модуль над кольцом коэффициентов R. Тогда подмножество $U = R[x]_{\leq m}$, состоящее из всех многочленов степени, не превосходящей m, является подмодулем в $R[x]$.

• Пусть $V = R[x_1, \ldots, x_n]$ — кольцо многочленов от n переменных, рассматриваемое как модуль над кольцом коэффициентов R. Обозначим через $R[x_1, \ldots, x_n]_m$ множество всех форм степени m, т.е. однородных многочленов степени m (напомним, что 0 является однородным любой степени).

§ 9$\diamondsuit$. Линейная оболочка системы векторов

Пусть как обычно V некоторый правый R-модуль. Сейчас мы свяжем с каждой системой векторов некоторый подмодуль в V.

Определение. Линейной оболочкой *векторов* $u_1, \dots, u_n \in V$ *— или* **подмодулем, порожденным** $u_1, \dots, u_n$ *— называется множество*

$$\langle u_1, \dots, u_n \rangle = L(u_1, \dots, u_n)$$

всех линейных комбинаций векторов $u_1, \dots, u_n$*:*

$$\langle u_1, \dots, u_n \rangle = \{u_1\lambda_1 + \ldots + u_n\lambda_n \mid \lambda_1, \dots, \lambda_n \in K\}.$$

Покажем, что $\langle u_1, \dots, u_n \rangle$ действительно подмодуль.

Предложение. *Для любых* $u_1, \dots, u_n \in V$ *их линейная оболочка*

$$U = \langle u_1, \dots, u_n \rangle$$

является подмодулем в V*. При этом* $U \leq V$ *может быть охарактеризован как наименьший подмодуль, содержащий векторы* $u_1, \dots, u_n$*.*

Доказательство. По самому определению любой подмодуль $W \leq V$, содержащий $u_1, \dots, u_n$, обязан содержать все линейное комбинации этих векторов, и, значит, $U \subseteq V$. Покажем теперь, что U — действительно подмодуль. В самом деле, пусть $u_1\lambda_1 + \ldots + u_n\lambda_n$ и $u_1\mu_1 + \ldots + u_n\mu_n$ суть линейные комбинации векторов $u_1, \dots, u_n$. Тогда

$$(u_1\lambda_1 + \ldots + u_n\lambda_n) + (u_1\mu_1 + \ldots + u_n\mu_n) = u_1(\lambda_1 + \mu_1) + \ldots + u_n(\lambda_n + \mu_n),$$

также является линейной комбинацией $u_1, \dots, u_n$. Аналогично, если $\lambda \in K$, то $\lambda(\lambda_1 u_1 + \ldots + \lambda_n u_n) = \lambda\lambda_1 u_1 + \ldots + \lambda\lambda_n u_n$. Тем самым, $U \leq V$.

В случае, когда $V = \langle u_1, \dots, u_n \rangle$, говорят что $u_1, \dots, u_n$ **порождают** V или что $u_1, \dots, u_n$ являются **системой образующих** для V.

Все сказанное выше обобщается и на бесконечные семейства векторов. В частности, можно определить линейную оболочку $L(u_i, i \in I)$ бесконечного семейства векторов $\{u_i\}$, $i \in I$. В случае, когда $R = K$ — поле, $\langle x_1, \dots, x_n \rangle$ называется подпространством, порожденным $x_1, \dots, x_n$.

Пусть $x \in V$. Ясно, что подмодуль порожденный элементом x, совпадает с множеством $xR = \{x\lambda \mid \lambda \in R\}$ всех его скалярных кратных. Подмодуль, порожденный одним элементом, называется **циклическим** и в дальнейшем мы полностью выясним структуру таких модулей.

Задача. Докажите, что

$$\langle x_1, \dots, x_n \rangle = x_1R + \ldots + x_nR.$$

§ 10$\diamondsuit$. Фактор-модуль

Пусть V правый R-модуль, а $U \leq V$ — подмодуль модуля V. В этом случае определена фактор-группа V/U. Напомним, что как множество V/U является фактор-множеством по отношению эквивалентности, задаваемому сравнимостью по модулю U:

$$u \equiv v \pmod U \quad \Longleftrightarrow \quad u - v \in U.$$

Так как U аддитивная подгруппа, сравнимость по модулю U действительно задает на V отношение эквивалентности. Классами этой эквивалентности являются **смежные классы** по модулю U,

$$v + U = \{v + u \mid u \in U\}, \qquad v \in V.$$

Класс $v + U$ называется классом элемента $v \in V$, любой такой v называется **представителем** этого класса. Два смежных класса либо не пересекаются, либо совпадают, В случае модулей такие смежные классы часто называются также **линейными подмногообразиями**, параллельными U. Фактор-группа V/U состоит из всех таких смежных классов,

$$V/U = \{v + U \mid v \in V\},$$

Группа V абелева, а U подгруппа, так что операция в V/U определяется сложением классов по Минковскому

$$(v + U) + (w + U) = (v + w) + (U + U) = (v + w) + U.$$

При таком определении не возникает никаких вопросов, связанных с **корректностью**, иными словами, независимостью результата от выбора представителей в смежных классах $v + U$ и $w + U$. Эта операция превращает V/U в абелеву группу.

Сейчас мы убедимся, что так как $U \leq V$ не просто подгруппа, а подмодуль, на этой V/U можно определить структуру R-модуля. Тогда для любого $\lambda \in R$ следующая выкладка

$$(v + U)\lambda = v\lambda + U\lambda = v\lambda + U$$

показывает, что класс $v\lambda + U$ не зависит от выбора представителя v.

Абелева группа V/U с так определенным правым действием R называется **фактор-модулем** V по U. В случае векторных пространств, естественно, говорят о **фактор-пространствах**. По самому построению фактор-модуля V/U отображение

$$\pi : V \longrightarrow V/U, \qquad v \mapsto v + U,$$

линейно. Это отображение называется **канонической проекцией** V на фактор-модуль V/U.

§ 11$\diamondsuit$. Ядро и образ линейного отображения

Пусть U, V — модули над R, а $\phi : U \longrightarrow V$ — линейное отображение. В настоящем параграфе мы свяжем с отображением ϕ подмодуль $\mathrm{Ker}(\phi)$ в U, называемый ядром ϕ и подмодуль $\mathrm{Im}(\phi)$ в V, называемый образом ϕ. Эти подмодули являются важнейшими геометрическими объектами, связанными с ϕ. Кроме того, мы рассмотрим соответствующие фактор-модули.

1. Образ и ядро линейного отображения. Образ ϕ — это обычный образ ϕ как отображения. Тем самым,

$$\mathrm{Im}(\phi) = \{\phi(x) \mid x \in U\} = \{y \in V \mid \exists x \in U, \phi(x) = y\}.$$

Ясно, что $\phi(U) \leq V$. В самом деле, $0 = \phi(0) \in \mathrm{Im}(\phi)$. Если $x, y \in \mathrm{Im}(\phi)$, то существуют $u, v \in H$ такие, что $\phi(u) = x$, $\phi(v) = y$. В силу линейности $\phi(u + v) = \phi(u) + \phi(v) = x + y$, так что $x + y \in \mathrm{Im}(\phi)$. По той же причине $\phi(\lambda u) = \lambda\phi(u) = \lambda x \in \mathrm{Im}(\phi)$.

Свяжем теперь с линейным отображением ϕ некоторый подмодуль в U.

Определение. Ядром *линейного отображения* $\phi : U \longrightarrow V$ *называется полный прообраз* 0*:*

$$\mathrm{Ker}(\phi) = \{x \in U \mid \phi(x) = 0\}.$$

Ясно, что $\mathrm{Ker}(\phi) \leq U$. В самом деле, если $u, v \in \mathrm{Ker}(\phi)$, то $\phi(u\alpha + v\beta) = \phi(x)\alpha + \phi(y)\beta = 0$ для любых $\alpha, \beta \in R$. Ядро измеряет отклонение линейного отображения ϕ от инъективности. Например, если $\mathrm{Ker}(\phi) = U$, то $\phi = 0$. С другой стороны, чем ядро меньше, тем отображение ϕ ближе к инъективному. В частности, ϕ в том и только том случае инъективно, или, что в данном случае то же самое, является **мономорфизмом**, когда $\mathrm{Ker}(\phi) = 0$.

2. Кообраз и коядро линейного отображения. Можно ввести понятия, двойственные к понятиям ядра и образа. Фактор-модуль $\mathrm{Coim}(\phi) = U/\mathrm{Ker}(\phi)$ называется **кообразом** линейного отображения ϕ. Теорема о гомоморфизме утверждает, что $\mathrm{Coim}(\phi) \cong \mathrm{Im}(\phi)$, поэтому для модулей понятие кообраза используется достаточно редко.

Гораздо большее самостоятельное значение имеет понятие коядра. А именно, **коядром** линейного отображения ϕ называется фактор-модуль

$$\mathrm{Coker}(\phi) = V/\mathrm{Im}(\phi).$$

Ясно, что коядро измеряет отклонение линейного отображения ϕ от сюръективности точно в том же смысле, в котором ядро измеряет отклонение от инъективности. А именно, ϕ в том и только том случае сюръективно — или, что то же самое, является **эпиморфизмом**, когда $\mathrm{Im}(\phi) = V$ или, что то же самое, $\mathrm{Coker}(\phi) = 0$.

3. График линейного отображения. Еще одно подпространство, связанное с линейным отображением, это его график. А именно, **графиком** линейного отображения $\phi : U \longrightarrow V$ называется пространство

$$\Gamma(\phi) = \{(u, v) \in U \oplus V \mid \phi(u) = v\}.$$

Обратно, для того, чтобы подпространство $W \leq U \oplus V$ было графиком некоторого линейного отображения $\phi : U \longrightarrow V$, необходимо и достаточно, чтобы из того, что $(0, v) \in W$ следовало, что $v = 0$.

§ 12♢. Теорема о гомоморфизме

Сейчас мы покажем, что как и для других алгебраических систем факторизация отображений замечательным образом согласована со структурой модуля. Следующая теорема является одним из наиболее типичных и характерных результатов общей алгебры. В полной общности, а именно, для групп с операторами, она была впервые сформулирована Эмми Нетер.

Пусть U, V — модули над R, а $\phi : U \longrightarrow V$ — линейное отображение.

Теорема о гомоморфизме. *Для любого гомоморфизма $\phi : U \longrightarrow V$ имеет место изоморфизм*

$$\operatorname{Im}(\phi) \cong U/\operatorname{Ker}(\phi).$$

Мы уже видели аналогичные результаты для групп и колец, поэтому можем особенно не вдаваться в детали. Тем не менее, вспомним, что вообще с *каждым* отображением $\phi : U \longrightarrow V$ связано его **ядро** $N(\phi)$, являющееся разбиением U на слои отображения ϕ. Эти слои являются классами эквивалентности $\sim$ определяемой условием

$$u \sim v \qquad \Longleftrightarrow \qquad \phi(u) = \phi(v).$$

В случае, когда ϕ линейно, слои являются в точности смежными классами по $\operatorname{Ker}(\phi)$. Кстати, это объясняет, почему мы называем ядром гомоморфизма слой, содержащий 0: в отличие от произвольных отображений для линейных отображений задание одного этого слоя однозначно определяет *все* остальные классы. В самом деле

$$\phi(u) = \phi(v) \quad \Longleftrightarrow \quad \phi(u - v) = \phi(u) - \phi(v) = 0$$

так что $u - v \in \operatorname{Ker}(\phi)$. Но это и значит, что $u + \operatorname{Ker}(\phi) = v + \operatorname{Ker}(\phi)$. Обратно, если $u + \operatorname{Ker}(\phi) = v + \operatorname{Ker}(\phi)$, то $u = v + x$ для некоторого $x \in \operatorname{Ker}(\phi)$, так что $\phi(u) = \phi(v + x) = \phi(v) + \phi(x) = \phi(v)$. Теперь у нас все готово, чтобы доказать теорему о гомоморфизме.

Доказательство. Как мы только что вспомнили, сопоставление

$$\overline{u} = u + \operatorname{Ker}(\phi) \mapsto \phi(u)$$

корректно определяет инъективное отображение $\overline{\phi} : U/\operatorname{Ker}(\phi) \longrightarrow V$, образ которого совпадает с $\operatorname{Im}(\phi)$. Для завершения доказательства теоремы нам остается лишь проверить, что $\overline{\phi}$ гомоморфизм. В самом деле, пользуясь определением произведения классов, определением $\overline{\phi}$ и тем, что ϕ — гомоморфизм, получаем

$$\overline{\phi}(\overline{u}+\overline{v}) = \overline{\phi}(\overline{u+v}) = \phi(u+v) = \phi(u)+\phi(v) = \overline{\phi}(\overline{u})+\overline{\phi}(\overline{v}),$$

что и завершает доказательство.

Следствие. *Если $\phi : U \longrightarrow V$ эпиморфизм, то $V \cong U/\operatorname{Ker}(\phi)$.*

Теорема. *Пусть $\phi : U \longrightarrow V'$ — гомоморфизм групп, а нормальные подгруппы $U \trianglelefteq V$, $U' \trianglelefteq V'$ таковы, что $\phi(U) \le U'$. Тогда ϕ индуцирует гомоморфизм*

$$\overline{\phi} : V/U \longrightarrow V'/U', \qquad \overline{\phi}(v+U) = \phi(v)+U'.$$

Доказательство. Прежде всего, необходимо проверить корректность этого определения. Для этого заметим, что если $u+U = v+U$, то по условию на ϕ имеем $\phi(u)-\phi(v) = \phi(x-y) \in U'$, так что $\phi(u)+U' = \phi(v)+U'$. Осталось убедиться в том, что $\overline{\phi}$ гомоморфизм. В самом деле,

$$\begin{aligned}\overline{\phi}((u+U)+(v+U)) = \overline{\phi}(u+v+U) = \\ \phi(u+v)+U' = \phi(u)+\phi(v)+U' = \\ (\phi(u)+U')+(\phi(v)+U') = \overline{\phi}(u+U)+\overline{\phi}(v+U).\end{aligned}$$

Следствие. *Если в условиях теоремы $U = \phi^{-1}(U')$, то гомоморфизм $\overline{\phi} : V/U \longrightarrow V'/U'$ инъективен. Если, кроме того, ϕ сюръективен, то $\overline{\phi}$ изоморфизм.*

Теорема фон Дика. *Для любых подмодулей $U \le V \le W$ имеет место изоморфизм*

$$(W/U)/(V/U) \cong W/V.$$

Доказательство. Обозначим через $\pi : W \longrightarrow W/V$ каноническую проекцию. Так как $U \le V = \operatorname{Ker}(\pi)$, π индукцирует гомоморфизм $\pi' : W/U \longrightarrow W/V$, $w+U \mapsto w+V$. Ядро этого гомоморфизма равно $\operatorname{Ker}(\pi)/U = V/U$. Осталось применить теорему о гомоморфизме.

§ 13◊. Сумма и пересечение подмодулей

В настоящем параграфе мы опишем верхнюю и нижнюю грань в решетке подмодулей относительно включения.

1. Сумма и пересечение двух подмодулей. Пусть V — модуль, а $U, W \leq V$ два подмодуля в V. **Пересечением** подмодулей U и W называется их теоретико-множественное пересечение $U \cap W$. Очевидно, что $U \cap W \leq V$.

Пусть $U, W \leq V$ два подмодуля в V. **Суммой** подмодулей U и W называется их сумма по Минковскому

$$U + W = \{u + w \mid u \in U, w \in W\}.$$

Легко видеть, что $U + W$ является подмодулем в V. В самом деле,

$$(u_1 + w_1) + (u_2 + w_2) = (u_1 + u_2) + (w_1 + w_2) \in U + W,$$
$$(u + w)\lambda = u\lambda + w\lambda \in U + W.$$

Пересечение и сумма двух подмодулей — это в точности их инфимум и супремум в решетке подмодулей относительно включения. Иными словами, пересечение двух подмодулей — это *наибольший* подмодуль, содержащийся в каждом из них, а сумма — *наименьший* подмодуль, содержащий каждый из них.

Следующий очевидный, но исключительно важный результат, известный профессионалам как `Noetherscher Isomorphiesatz`, утверждает, что противоположные стороны параллелограмма равны.

Теорема Нетер об изоморфизме. *Для любых двух подмодулей* $U, V \leq W$ *имеет место изоморфизм*

$$(U + V)/U \cong V/(U \cap V).$$

Доказательство. В самом деле, гомоморфизм

$$V \mapsto (U + V)/U, \qquad v \mapsto v + U,$$

сюръективен, а его ядро равно $U \cap V$. Осталось сослаться на теорему о гомоморфизме.

Задача (модулярный закон). Докажите, что для любых трех подмодулей X, Y, Z модуля V таких, что $X \leq Y$, выполняется $Y \cap (X \cap Z) = X + (Y \cap Z)$.

2. Сумма и пересечение семейства подмодулей. Вообще, пусть U_i, $i \in I$, — произвольное семейство подмодулей в V. Тогда теоретико-множественное пересечение $\bigcap U_i$, $i \in I$, является подмодулем в V.

Вообще, пусть U_i, $i \in I$, — произвольное семейство подмодулей в V. Мх суммой называется подмодуль $\sum U_i$, $i \in I$, в V, состоящий из всех *конечных* сумм элементов из U_i. Иными словами, $\sum U_i$, $i \in I$, определяется следующим образом

$$\sum_{i \in I} U_i = \{\textstyle\sum u_i \mid \forall i \in I, u_i \in U_i \quad \& \quad u_i = 0 \text{ для почти всех } i\}$$

Точно так же, как выше, проверяется, что $\sum U_i$, $i \in I$, является подмодулем в V.

§ 14$\diamondsuit$. Прямые суммы и проекторы

В настоящем параграфе мы изучим самую простую — и *поэтому* самую важную — конструкцию, позволяющую строить новые модули из уже имеющихся.

1. Внешняя и внутренняя прямая сумма. В § 3 нам уже встречалось понятие внешней прямой суммы модулей. Пусть U и V два правых R-модуля. Тогда их **внешней прямой суммой** называется модуль $U \oplus V$, который как множество совпадает с декартовым произведением

$$U \times V = \{(u, v) \mid u \in U, v \in V\},$$

а операции определяются покомпонентно:

$$(u_1, v_1) + (u_2, v_2) = (u_1 + u_2, v_1 + v_2), \qquad (u, v)\lambda = (u\lambda, v\lambda).$$

В действительности, при обсуждении линейных отображений и матриц мы увидим, что для *правых* модулей было бы естественно записывать элементы $U \times V$ не строками, а столбцами, в виде

$$U \times V = \left\{ \begin{pmatrix} u \\ v \end{pmatrix} \;\middle|\; u \in U, v \in V \right\}.$$

Однако, из чисто типографских соображений мы придерживаемся традиционной формы записи.

С другой стороны модуль W называется **внутренней прямой суммой** своих подмодулей $U, V \leq W$, если выполняются два следующих условия:

$$U + V = W, \qquad U \cap V = 0.$$

Следующий результат утверждает, что внутренняя прямая сумма канонически изоморфна внешней.

Теорема. *Если модуль W является внутренней прямой суммой оих подгрупп $U, V \leq W$, то сопоставление*

$$\phi : U \oplus V \longrightarrow W, \qquad (u, v) \mapsto u + v$$

является изоморфизмом.

Доказательство. Легко видеть, что так определенное отображение ϕ линейно. В самом деле, следующая выкладка доказывает аддитивность:

$$\phi((u_1, v_1) + (u_2, v_2)) = \phi((u_1 + u_2, v_1 + v_2)) = (u_1 + u_2) + (v_1 + v_2) = \\ (u_1 + v_1) + (u_2 + v_2) = \phi(u_1, v_1) + \phi(u_2, v_2)$$

Точно так же проверяется и однородность:

$$\phi((u, v)\lambda) = \phi(u\lambda, v\lambda) = u\lambda + v\lambda = (u + v)\lambda = \phi(u, v)\lambda.$$

Равенство $U+V=W$ показывает, что ϕ сюръективно. Наконец, если $\phi(u,v)=u+v=0$, то $u=-v\in U\cap V=0$, так что отображение ϕ инъективно. Но это и значит, что ϕ изоморфизм.

2. Вложения и проекции. С разложением в прямую сумму связано несколько линейных отображений. А именно, определим вложения

$$\iota_U : U \longrightarrow U\oplus V,\quad u\mapsto (u,0),\qquad \iota_V : V \longrightarrow U\oplus V,\quad v\mapsto (0,v),$$

и проекции

$$\pi_U : U\oplus V \longrightarrow U,\quad (u,v)\mapsto u,\qquad \pi_V : U\oplus V \longrightarrow V,\quad (u,v)\mapsto v.$$

Легко видеть, что вложения и проекции удовлетворяют следующим равенствам

$$\pi_U\iota_U=\mathrm{id}_U,\quad \pi_U\iota_V=0,\quad \pi_V\iota_U=0,\quad \pi_V\iota_V=\mathrm{id}_V,$$

и, при композиции в обратном направлении,

$$\iota_U\pi_U+\iota_V\pi_V=\mathrm{id}_{U\oplus V}\,.$$

Все эти равенства удобнее всего переписать в матричном виде

$$\begin{pmatrix}\pi_U\\ \pi_V\end{pmatrix}(\iota_U,\iota_V)=\begin{pmatrix}\mathrm{id}_U & 0\\ 0 & \mathrm{id}_V\end{pmatrix},\qquad (\iota_U,\iota_V)\begin{pmatrix}\pi_U\\ \pi_V\end{pmatrix}=\mathrm{id}_{U\oplus V}\,.$$

В действительности эти равенства характеризуют прямые суммы. Если у нас есть модуль W и четыре отображения

$$\iota_U : U\longrightarrow W,\quad \iota_V : V\longrightarrow W,\quad \pi_U : W\longrightarrow U,\quad \pi_V : W\longrightarrow V,$$

удовлетворяющие сформулированным выше условиям, то $W\cong U\oplus V$.

3. Дополнение. Пусть $U\le W$. Подмодуль V называется **дополнением** к U в W, если $U\oplus V=W$, иными словами, если $U+V=W$ и $U\cap V=0$. Иногда эмфатически говорят о **прямых дополнениях**, чтобы отличить их от дополнений, удовлетворяющих различным добавочным условиям, таких, как инвариантные дополнения, ортогональные дополнения и т.д. Когда U фиксировано, подмодуль V называется также **дополнительным подмодулем** или, в случае векторных пространств, **дополнительным пространством**.

Теорема. *Пусть V — дополнение U в W Отображение*

$$V\mapsto W/U,\qquad v\mapsto v+U$$

является изоморфизмом.

Эта теорема показывает, что все дополнения к одному и тому же подмодулю изоморфны и с точки зрения линейной алгебры одинаково расположены по отношению к U.

Следствие. *Если V_1 и V_2 два дополнения к U в W, то отношение сравнимости по модулю U является биекцией между V_1 и V_2, устанавливающей изоморфизм между ними.*

Построенный в следствии изоморфизм называется **проектированием** V_1 на V_2 параллельно U.

4. Сумма и пересечение. Вложение

$$U \cap V \longrightarrow U \oplus V, \qquad u \mapsto (u, -u),$$

и проекция

$$U \oplus V \longrightarrow U + V, \qquad (u, v) \mapsto u + v,$$

объединяются в одну точную последовательность

$$0 \longrightarrow U \cap V \longrightarrow U \oplus V \longrightarrow U + V \longrightarrow 0,$$

5. Проекторы. Линейный оператор $\phi : V \longrightarrow V$ называется **проектором**, если он **идемпотентен**, $\phi^2 = \phi$. Пусть $V = V_1 \oplus \ldots \oplus V_s$ есть разложение V в прямую сумму. Тогда каждый $v \in V$ однозначно представляется в виде $v = v_1 + \ldots + v_s$, где $v_i \in V_i$. Легко видеть, что проекции на прямые слагаемые

$$\phi_i : V \longrightarrow V_i, \qquad v \mapsto v_i,$$

обладают следующими свойствами.

- $\phi_i^2 = \phi_i$
- $\phi_i \phi_j = 0$ при $i \neq j$
- $\phi_1 + \ldots + \phi_s = \mathrm{id}_V$

Теорема. *Любое семейство проекторов с перечисленными свойствами задает разложение V в прямую сумму*

$$V = \mathrm{Im}(\phi_1) \oplus \ldots \oplus \mathrm{Im}(\phi_n).$$

§ 15♠. Прямые суммы и прямые произведения

Для конечного числа множителей внутренняя и внешняя точка зрения на прямое произведение совпадают. Однако для бесконечного числа множителей они начинают различаться. В настоящем параграфе мы опишем две конструкции, обобщающие прямую сумму на случай произвольного семейства модулей.

1. Прямое произведение. Пусть теперь V_i, $i \in I$, — произвольное семейство R-модулей.

Определение. *Множество* $\prod\limits_{i\in I} V_i$ *или, если индексное множество* I *однозначно определено контекстом, просто* $\prod V_i$ *вместе с покомпонентными операциями*

$$(u_i)+(v_i)=(u_i+v_i),\qquad (u_i)\lambda=(u_i\lambda),$$

называется **прямым произведением** *модулей* V_i.

Прямое произведение сразу возникает вместе с **каноническими проекциями**

$$\mathrm{pr}_j:\prod V_i\longrightarrow V_j,\qquad (v_i)\mapsto v_j,$$

на индивидуальные множители.

В дальнейшем нам понадобится чуть другая вербализация конструкции прямого произведения. А именно, мы будем истолковывать $\prod V_i$ как множество таких функций $I\mapsto\bigcup V_i$, для которых $f(i)\in V_i$ для каждого $i\in I$. На множестве всех таких функций вводится обычный операции на функциях, которые превращают его в R-модуль. С этой точки зрения каноническая проекция на j-й множитель — это просто сопоставление функции f ее значения в точке j.

2. Прямая сумма. Особенно важен частный случай конструкции ограниченного прямого произведения, получающийся при $H_i=1$.

Определение. *Множество*

$$\bigoplus V_i=\{(v_i)\mid v_i\in V_i,\ v_i=0\ \text{для почти всех}\ i\}\leq\prod_{i\in I}V_i$$

вместе с покомполнетными операциями

$$(u_i)+(v_i)=(u_i+v_i),\qquad (u_i)\lambda=(u_i\lambda),$$

называется **прямой суммой** *модулей* V_i.

Прямая сумма часто обозначается также $\coprod V_i$ и называется **копроизведением** модулей V_i. Прямая сумма сразу возникает вместе с координатными вложениями

$$\mathrm{incl}_j:G_j\longrightarrow\bigoplus V_i,\qquad v_j\mapsto(v_i),$$

индивидуальных слагаемых.

Таким образом, по определению $\bigoplus V_i$ состоит из всех функций $f:I\longrightarrow\bigcup V_i$ таких, что $f(i)\in V_i$ *с конечным носителем*, т. е. таких, что $f(i)=0$ для всех i, кроме конечного их числа. В частности, если только конечное число среди модулей V_i отлично от 1 — например, для конечного числа слагаемых — прямая сумма совпадает с прямым произведением.

Глава 2. СВОБОДНЫЕ И ПРОЕКТИВНЫЕ МОДУЛИ

Будьте мудры как змеи и просты как голуби.
Иисус из Назарета

В настоящей главе мы изучаем важнейшие классы модулей, промежуточные между классом всех модулей, которым мы занимались в предыдущей главе, и классом векторных пространств, который мы детально рассмотрим в следующей главе.

Самая знаменитая аксиома математики, **аксиома выбора**, утверждает, что в каждом векторном пространстве существует базис. Для модулей над кольцом это, вообще говоря, совершенно не так. Тем не менее, над любым кольцом мы можем рассмотреть **свободные модули**, в которых **базис** действительно существует. В учебных целях и некоторых элементарных приложениях можно даже ограничиться этим классом модулей.

Но в *серьезных* приложениях сделать это не удастся, так как не только в произвольных подмодулях, но даже в прямых слагаемых свободных модулей никаких базисов, вообще говоря, нет. Оказывается, однако, что большинство реально используемых в линейной алгебре вычислительных методов опирается не на существование базисов, а на существование координат. Конечно, выбор базиса определяет координаты векторов. Оказывается, однако, что часто выбор линейно зависимой системы образующих тоже позволяет корректно определить координаты. Модули, в которых существуют **координатные системы**, называются **проективными**, и именно они доставляют естественную общность, в которой следует развивать линейную алгебру.

• С одной стороны, на проективные модули без большого труда переносится весь обычный классический аппарат линейной алгебры.

• С другой стороны, класс проективных модулей достаточен для большинства обычных приложений линейной алгебры в анализе, геометрии, топологии и теории дифференциальных уравнений.

Тем не менее, в силу врожденной застенчивости, я не решился последовательно встать на современную точку зрения, основанную на понятии проективного модуля, и веду большую часть изложения в традиционном контексте свободных модулей.

§ 1♢. Линейная зависимость и независимость

В настоящем параграфе мы продолжаем считать, что V — правый R-модуль.

1. Линейная зависимость и независимость. Сейчас мы введем **ключевое** понятие всей линейной алгебры.

Определение. *Векторы $u_1, \dots, u_n \in V$ называются* **линейно независимыми***, если любая их нетривиальная линейная комбинация отлична от 0, иными словами, если из того, что хотя бы один из коэффициентов $\lambda_1, \dots, \lambda_n \in K$ не равен 0, вытекает, что $u_1\lambda_1 + \ldots + u_n\lambda_n \neq 0$*

Это определение можно прочесть и следующим образом: любая линейная комбинация векторов $u_1\lambda_1 + \ldots + u_n\lambda_n$, равная 0, **тривиальна**, т.е. все ее коэффициенты равны 0:

$$u_1\lambda_1 + \ldots + u_n\lambda_n = 0 \quad \Longrightarrow \quad \lambda_1 = \ldots = \lambda_n = 0.$$

Отметим, в частности, что пустая система векторов линейно независима.

Векторы, не являющиеся линейно независимыми, называются **линейно зависимыми**. Чтобы векторы $u_1, \dots, u_n$ были линейно зависимы, необходимо и достаточно, чтобы существовали такие коэффициенты $\lambda_1, \dots, \lambda_n \in R$, не все равные 0, что $u_1\lambda_1 + \ldots + u_n\lambda_n = 0$. Любое равенство такого вида, в котором не все коэффициенты равны 0, называется **нетривиальным линейным соотношением** между векторами $u_1, \dots, u_n$. Между линейно независимыми векторами существует только тривиальное линейное соотношение $u_1 0 + \ldots + u_n 0 = 0$. Следующее утверждение очевидно.

Лемма. *Любая подсистема линейно независимой системы векторов сама линейно независима.*

Эту лемму можно сформулировать еще и так: любая надсистема линейно зависимой системы линейно зависима.

2. Принцип компактности линейной независимости. Определение линейной независимости без труда обобщается на любое бесконечное семейство векторов $\{u_\alpha\}$, $\alpha \in \Omega$. Для этого вспомним, что по определению линейная комбинация бесконечного семейства — это линейная комбинация какого-то его конечного подсемейства. Это значит, что если какая-то нетривиальная линейная комбинация семейства $\{u_\alpha\}$ равна 0, то в $\{u_\alpha\}$ найдется какое-то **конечное** подсемейство векторов $u_1, \dots, u_n$ и его нетривиальная линейная комбинация, равная 0. Тем самым, в любом линейно зависимом семействе найдется конечное линейно зависимое подсемейство. Таким образом, мы можем сформулировать **принцип компактности линейной независимости**: семейство, **любое** конечное подсемейство которого линейно независимо, само будет линейно независимым.

3. Первые примеры. Приведем несколько простейших примеров.

• **Нулевой вектор.** Любое семейство, содержащее вектор $u = 0$, линейно зависимо: достаточно взять в качестве коэффициентов линейной комбинации 1 при векторе u и 0 при всех остальных векторах.

• **Коллинеарность.** Два вектора u, v на плоскости тогда и только тогда линейно зависимы, когда они коллинеарны, т.е. лежат на одной прямой. В частности, любые два вектора на прямой линейно зависимы.

• **Компланарность.** Три вектора u, v, w в трехмерном пространстве тогда и только тогда линейно зависимы, когда они компланарны, т.е. лежат в одной плоскости. В частности, любые три вектора на плоскости линейно зависимы.

• Пусть K — поле. Тогда любые $\geq n+1$ штук векторов в пространстве K^n линейно зависимы. Эту мысль обычно выражают чуть иначе, говоря, что пространство K^n является n-мерным.

• Функции $x \mapsto \cos^2(x)$, $x \mapsto \cos(2x)$ и $x \mapsto 1$, линейно зависимы. В самом деле, $2\cos^2(x) - \cos(2x) - 1 = 0$ есть равная 0 нетривиальная линейная комбинация этих функций с коэффициентами $2, -1, -1$. В то же время функции $x \mapsto \cos^2(x)$, $x \mapsto \cos(x)$ и $x \mapsto 1$, линейно независимы.

• **Стандартный базис пространства столбцов.** Вернемся к примеру, рассмотренному в предыдущей главе. Пусть $e_1, \ldots, e_n$ — стандартный базис пространства столбцов K^n. Тогда векторы $e_1, \ldots, e_n$ образуют линейно независимую систему. В самом деле, если для некоторых коэффициентов $\lambda_1, \ldots, \lambda_n \in K$ имеем $u_1\lambda_1 + \ldots + u_n\lambda_n = (\lambda_1, \ldots, \lambda_n)^t = 0$, то $\lambda_1 = \ldots = \lambda_n = 0$.

• **Стандартные мономы.** Рассмотрим пространство $V = K[t]$. Тогда семейство $1, x, \ldots, x^n, \ldots$ линейно независимо. В силу принципа компактности достаточно доказать это для любого **конечного** семейства стандартных мономов, а любое конечное семейство содержится в некотором семействе вида $1, x, \ldots, x^n$. Пусть $\lambda_0, \ldots, \lambda_n \in K$ таковы, что $1\lambda_0 + x\lambda_1 + \ldots + x^n\lambda_n = 0$. В силу определения равенства многочленов это означает, что $\lambda_1 = \ldots = \lambda_n = 0$.

§ 2♢. Базис свободного модуля, координаты

Сейчас мы введем одно из центральных понятий всей линейной алгебры.

Определение. *Система векторов $v_1, \ldots, v_n$ называется* **базисом** *модуля V, если*

B1 *система $v_1, \ldots, v_n$* **линейно независима**;

B2 *система $v_1, \ldots, v_n$* **порождающая**, *т.е. все пространство совпадает с ее линейной оболочкой.*

Без всяких изменений понятие базиса переносится и на случай бесконечных систем. Мы доказываем следующую теорему для конечных базисов, но она без всяких изменений переносится и на бесконечные.

Теорема. *Для системы векторов м $v_1, \ldots, v_n \in V$ следующие условия эквивалентны:*

(1) *$v_1, \ldots, v_n$ — базис,*

(2) *каждый вектор $v \in V$, единственным образом представляется в виде линейной комбинации векторов $v_1, \ldots, v_n$.*

Доказательство. (1) $\Longrightarrow$ (2) Пусть $v_1, \ldots, v_n$ — базис модуля V. По определению любой вектор $v \in V$ является линейной комбинацией векторов $v_1, \ldots, v_n$. Почему такое представление единственно? Пусть $v =$

$v_1\lambda_1+\ldots+v_n\lambda_n$ и $v = v_1\mu_1+\ldots+v_n\mu_n$ — два представления одного и того же вектора v как линейной комбинации $v_1,\ldots,v_n$. Тогда, вычитая эти выражения, получим $v_1(\lambda_1-\mu_1)+\ldots+v_n(\lambda_n-\mu_n) = 0$, и, так как векторы $v_1,\ldots,v_n$ линейно независимы, то эта линейная зависимость должны быть тривиальна, так что все ее коэффициенты нулевые, $\lambda_1-\mu_1 = \ldots = \lambda_n-\mu_n = 0$. Но это как раз и значит, что выражение v как линейной комбинации $v_1,\ldots,v_n$ единственно.

(2) $\Longrightarrow$ (1) Очевидно, что условие (2) сильнее условия (1): линейная независимость системы $v_1,\ldots,v_n$ эквивалентна утверждению о том, что *нулевой* вектор допускает единственное представление как линейная комбинация векторов $v_1,\ldots,v_n$, а в условии (2) то же самое утверждается для *любого* вектора.

Таким образом, если $v_1,\ldots,v_n$ — базис модуля V, то для любого вектора $v\in V$ однозначно определены скаляры $\lambda_1,\ldots,\lambda_n\in K$ такие, что $v = v_1\lambda_1+\ldots+v_n\lambda_n$. Они называются **координатами** вектора v в базисе $v_1,\ldots,v_n$, а составленный из них столбец $(\lambda_1,\ldots,\lambda_n)^T$ — **столбцом координат**. Важно четко понимать, что этот КООРДИНАТНЫЙ СТОЛБЕЦ ЗАВИСИТ ОТ ВЫБОРА БАЗИСА.

Приведем несколько примеров базисов и соответствующих координат.

• **Единичные орты.** Пусть $V = \mathbb{R}^3$ — обычное трехмерное эвклидово пространство, i,j,k — координатные орты, направленные по декартовым осям. Тогда i,j,k — базис пространства V, (каждый вектор $v\in V$ однозначно представляется в виде $v = \alpha i+\beta j+\gamma k$), а координаты α,β,γ вектора $v\in V$ в этом базисе — это просто проекции v на координатные оси.

• **Стандартный базис пространства столбцов.** Более общо, пусть $V = K^n$ — пространство столбцов высоты n над K. Тогда построенный выше 'стандартный базис' $e_1,\ldots,e_n$ действительно является базисом пространства K^n (это линейно независимая порождающая система), причем i-я координата столбца $v = (\alpha_1,\ldots,\alpha_n)^T$ в этом базисе — это просто его i-я компонента как столбца: $(a_1,\ldots,a_n) = a_1e_1+\ldots+a_ne_n$.

• **Стандартный базис $\mathbb{C}$.** Пусть $K = \mathbb{R}$, $V = \mathbb{C}$. Тогда стандартный выбор базиса $\mathbb{C}$ как векторного пространства над $\mathbb{R}$ это $1, i$. Координаты комплексного числа $z\in\mathbb{C}$ в этом базисе — это просто его вещественная и мнимая часть, соответственно: $z = \mathrm{re}(z)1+\mathrm{im}(z)i$.

• **Стандартный базис $\mathbb{H}$.** Пусть $K = \mathbb{R}$, $V = \mathbb{H}$. Тогда стандартный выбор базиса $\mathbb{H}$ как векторного пространства над $\mathbb{R}$ это $1, i, j, k$. Если считать, что $\mathbb{C}$ порождено 1 и i над $\mathbb{R}$, то в качестве базиса $\mathbb{H}$ над $\mathbb{C}$ можно взять 1 и j.

• **Базис $\mathbb{Q}(\sqrt{2})$.** Рассмотрим вещественное квадратичное поле $\mathbb{Q}(\sqrt{2})$, получающееся из $\mathbb{Q}$ присоединением квадратного корня из 2: $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$. Тогда в качестве базиса этого пространства можно взять 1 и $\sqrt{2}$, а координатами числа $x = a+b\sqrt{2} = a1+b\sqrt{2}$ как раз и будут a и b.

• **Стандартные матричные единицы.** Рассмотрим $V = M(m,n,K)$ как векторное пространство над K. Тогда стандартные матричные единицы e_{ij}, $1 \le i \le m$, $1 \le j \le n$, образуют базис V. Напомним, что стандартная матричная единица e_{ij} — это матрица, у которой в позиции (i,j) стоит 1 и нули во всех остальных позициях, поэтому координаты матрицы $x = (x_{ij})$, $1 \le i \le m$, $1 \le j \le n$, в этом базисе совпадают с ее матричными элементами x_{ij}.

Рассмотрим теперь несколько примеров бесконечномерных пространств.

• **Стандартные мономы.** Пусть $V = K[x]$ — кольцо полиномов от одной переменной над K. Рассматриваемое как векторное пространство над K оно имеет базис $1, x, x^2, \ldots$, координаты в этом базисе — это в точности коэффициенты многочлена, почти все они равны 0.

• **Базис Гамеля.** Пусть $K = \mathbb{Q}$, $V = \mathbb{R}$. Как мы вскоре покажем, в любом векторном пространстве существует базис, в частности, $\mathbb{R}$ имеет базис как векторное пространство над $\mathbb{Q}$. В то же время явно указать такой базис (называемый **базисом Гамеля**, в отличие от 'базисов', используемых в функциональном анализе) нет никакой возможности.

• **Стандартные экспоненциальные мономы.** В любом стандартном курсе теории дифференциальных уравнений доказывается, что стандартные экспоненциальные мономы $x^n e^{ax}$, где $n \in \mathbb{N}_0$, $a \in \mathbb{C}$, образуют базис кольца экспоненциальных многочленов $\mathrm{Expo}_{\mathbb{C}}$ как векторного пространства над $\mathbb{C}$.

• **Простейшие дроби.** Во втором семестре мы докажем, что рациональные дроби вида $(x-c)^{-m}$, где $c \in \mathbb{C}$, $m \in \mathbb{N}$, образуют базис кольца правильных рациональных дробей как векторного пространства над $\mathbb{C}$. Отсюда следует, что стандартные мономы $1, x, x^2, \ldots$ и дроби вида $(x-c)^{-m}$ образуют базис поля $K(x)$ рациональных дробей как векторного пространства над $\mathbb{C}$.

Комментарий. *Первое*, чему должен научиться каждый серьезный студент при изучении линейной алгебры, состоит в понимании того, что все базисы векторного пространства эквивалентны и конкретный выбор одного из них не имеет **никакого** значения. *Второе*, чему он должен научиться — это пониманию того, что некоторые базисы **гораздо** удобнее для вычислений, чем некоторые другие, причем не всегда удобнее пользоваться теми базисами, которые *кажутся* наиболее естественными.

Задача. Рассмотрите поле $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ как векторное пространство над $\mathbb{Q}$. У этого пространства есть очевидный базис $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. Докажите, что в качестве базиса этого пространства можно взять $1, \sqrt{5+2\sqrt{6}}, 5 + 2\sqrt{6}, \sqrt{5+2\sqrt{6}}^3$.

В течение второго и третьего семестра нам постепенно станет ясно, что для большинства вычислений построенный в этой задаче **степенной базис** оказывается значительно удобнее.

• Пусть $\iota : R \hookrightarrow S$ — расширение колец, а V — свободный S-модуль. Если S свободный R-модуль, то R-модуль ${}_{\iota}V$, получающийся из V сужением скаляров, является свободным R-модулем. В самом деле, если e_i — базис V над S, а α_j — базис S над R, то $e_i\alpha_j$ — базис V над R (проверьте это!)

§ 3♢. Формальные линейные комбинации

Пусть X — произвольное множество, а R — коммутативное кольцо с 1. Сейчас мы покажем, что X можно рассматривать как базис некоторого R-модуля. Эта конструкция используется весьма часто, как сама по себе, так и как начальный фрагмент многих математических конструкций.

Часто говорят о *формальных* линейных комбинациях элементов X с коэффициентами из R. Это значит, что мы строим модуль, в котором все элементы $x \in X$ являются *линейно независимыми* и рассматриваем линейные комбинации этих элементов. Проще всего построить такой модуль следующим образом. Рассмотрим множество $R^{(X)}$ *финитных* функций $X \longrightarrow R$, т.е. таких функций $f : X \longrightarrow R$, что $f(x) = 0$ для всех $x \in X$, кроме конечного их числа. На множестве $R^{(X)}$ определены обычные покомпонентные сложение функций $(f + g)(x) = f(x) + g(x)$ и умножение на скаляр $(\lambda f)(x) = \lambda f(x)$. Каждому $x \in X$ соответствует δ-функция $\delta_x : X \longrightarrow R$, $\delta_x(y) = 1$, если $y = x$, $\delta_x(y) = 0$, $y \neq x$.

Теорема. *Для каждого множества X существует свободный правый R-модуль $V = R^{(X)}$ с базисом X.*

Эта конструкция используется в алгебре очень часто.

• Как R-модуль кольцо многочленов состоит из формальных линейных комбинаций стандартных мономов x^n, $n \in \mathbb{N}_0$, с коэффициентами из R.

• Вообще, если M — любой моноид (например, группа), то как модуль моноидная алгебра $R[M]$ состоит из формальных линейных комбинаций элементов M, с коэффициентами из R.

• Пусть e_{ij}, $1 \leq i \leq m$, $1 \leq j \leq n$, — стандартные матричные единицы. Тогда модуль $m \times n$-матриц $M(m, n, R)$ можно было бы определеить как модуль формальных линейных комбинаций e_{ij}.

• В главе 4 мы будем широко пользоваться конструкциями в духе следующей. Пусть V — некоторый R-модуль. Положим $X = V$ и рассмотрим R-модуль $Z = R^{(V)}$. Иными словами, элементами модуля Z являются линейные комбинации $\sum v\lambda_v$ элементов $v \in V$ — но, конечно, не их настоящие линейные комбинации как элементов V, а *формальные* линейные комбинации! После этого мы можем наложить на элементы v какие-то соотношения — конечно, не все соотношения, выполняющиеся в V, а какую-то их часть, или какие-то другие соотношения. Такого рода конструкции часто используются для того, чтобы строить различные большие, чем сам V модули.

§ 4♢. Универсальное свойство базиса

В настоящем параграфе мы дадим еще одно определение базиса. Фактически во многих приложениях используется именно универсальное свойство базиса: ЛИНЕЙНОЕ ОТОБРАЖЕНИЕ ОДНОЗНАЧНО ОПРЕДЕЛЯЕТСЯ СВОИМИ ЗНАЧЕНИЯМИ НА БАЗИСЕ, ПРИЧЕМ ЭТИ ЗНАЧЕНИЯ МОГУТ БЫТЬ ПРОИЗВОЛЬНЫМИ.

1. Универсальное свойство базиса. Следующий результат объясняет *смысл* понятия базиса.

Теорема. *Пусть $v_1, \ldots, v_n$ базис свободного R-модуля V. Далее, пусть U произвольный R-модуль и $x_1, \ldots, x_n \in U$. Тогда существует единственное линейное отображение $\phi : V \longrightarrow U$ такое, что $\phi(v_i) = x_i$.*

Доказательство. Существование. Пусть $v \in V$. Тогда v допускает единственное представление в виде $v = v_1\lambda_1 + \ldots + v_n\lambda_n$. Положим

$$\phi(v) = x_1\lambda_1 + \ldots + x_n\lambda_n.$$

Ясно, что этим задано R-линейное отображение $V \longrightarrow U$ — проверьте это!

Единственность. Пусть теперь $\psi : V \longrightarrow U$ произвольное R-линейное отображение такое, что $\psi(v_i) = x_i$. Пусть снова $v = v_1\lambda_1 + \ldots + v_n\lambda_n$. Из R-линейности вытекает, что $\psi(v) = x_1\lambda_1 + \ldots + x_n\lambda_n$.

Следствие. *Для каждого модуля U существвет свободный модуль V и эпиморфизм $V \longrightarrow U$.*

Доказательство. Возбмем любую систему образующих x_i, $i \in I$, модуля U и рассмотрим свободный модуль V_i

2. Изоморфизм свободных модулей. Следующая лемма утверждает, что инъективные линейные отображения сохраняют свойство системы векторов быть линейно независимой, а сюръективные линейные отображения сохраняют свойство системы векторов быть порождаюшей системой.

Лемма. *Пусть $\phi : U \longrightarrow V$ — R-линейное отображение, $x_1, \ldots, x_n \in R$.*

- *Если ϕ инъективно, и векторы $x_1, \ldots, x_n$ линейно независимы, то их образы $\phi(x_1), \ldots, \phi(x_n)$ тоже линейно независимы.*
- *Если ϕ сюръективно и $U = \langle x_1, \ldots, x_n\rangle$, то $V = \langle \phi(x_1), \ldots, \phi(x_n)\rangle$.*

Доказательство. Для доказательства первого утверждения предположим, что $\phi(x_i)$ линейно зависимы. Пусть $\phi(x_i)\alpha_i = 0$ линейная зависимость между ними. В силу линейности ϕ имеем

$$\phi(\sum x_i\alpha_i) = \sum \phi(x_i)\alpha_i = 0.$$

Воспользовавшись теперь инъективностью ϕ мы получим линейную зависимость $\sum x_i\alpha_i = 0$ между x_i. Так как по условию $x_1, \ldots, x_n$ линейно независимы, эта линейная зависимость тривиальна, $\alpha_1 = \ldots = \alpha_n = 0$.

Для доказательства второго утверждения возьмем какое-то $y \in V$. В силу сюръективности ϕ найдется $x \in U$ такое, что $\phi(x) = y$. Так как $x_1, \ldots, x_n$ порождают U, вектор x можно представить в виде их линейной комбинации $x = \sum x_i\alpha_i$. Но тогда в силу линейности ϕ

$$y = \phi(x) = \phi(\sum x_i\alpha_i) = \sum \phi(x_i)\alpha_i,$$

как и утверждалось.

Теорема. *Два свободных модуля в том и только том случае изоморфны, когда в них существуют базисы одинаковой мощности.*

Доказательство. Предположим, что в модулях U и V существуют базисы $u_1, \dots, u_n$ и $v_1, \dots, v_n$ одинаковой мощности. В силу универсального свойства базиса существует единственное линейное отображение $\phi : U \longrightarrow V$ такое, что $\phi(u_i) = v_i$ для всех $1 \le i \le n$. Так как векторы $v_1, \dots, v_n$ порождают V, это отображение сюръективно. С другой стороны, так как $u_1, \dots, u_n$ линейно независимы, ядро этого отображения равно 0.

Обратно, пусть $u_1, \dots, u_n$ — базис U, а $\phi : U \longrightarrow V$ — изоморфизм. Мы утверждаем, что тогда векторы $\phi(u_1), \dots, \phi(u_n)$ образуют базис V. В самом деле, так как ϕ инхективно, то по предыдущей лемме эти векторы линейно независимы, а так как ϕ сюръективно, то они порождают V.

Стоит предостеречь начинающего, что из этой теоремы совершенно не вытекает, что *все* базисы свободного модуля обязаны иметь одинаковую мощность! Это, вообще говоря, совершенно не так и в двух следующих параграфах мы обсудим вопрос о том, в какой степени ранг свободного модуля определен однозначно.

3. Выделение свободного модуля прямым слагаемым. Проиллюстрируем универсальное свойство базиса еще на одном важнейшем примере.

Теорема. *Пусть $\phi : U \longrightarrow V$ — сюръективное линейное отображение, причем модуль V свободен. Тогда существует линейное отображение $\psi : V \longrightarrow U$ такое, что $\phi \circ \psi = \mathrm{id}_V$.*

Доказательство. Пусть $v_1, \dots, v_n$ — базис V. В силу сюръективности отображения ϕ существуют $x_1, \dots, x_n$ такие, что $\phi(x_i) = v_i$. В силу универсального свойства базиса существует единственное линейное отображение $\psi(v_i) = x_i$. По самому определению $\phi(\psi(v_i)) = v_i$, а так как v_i порождают V, то $\phi \circ \psi = \mathrm{id}_V$, как и утверждалось.

§ 5♡. Единственность ранга

> Если это доказательство не является строгим, достаточно, чтобы оно было удовлетворительным. Мы сможем найти строгое доказательство позже, после того, как изучим то, что оставили в стороне сейчас, как требующее слишком долгих исследований.
>
> Платон, *Алкивиад*, XXV

Из теоремы Штейница, которую мы докажем в следующей главе, вытекает, что размерность векторного пространства определена однозначно. Отсюда сразу следует, что ранг свободного модуля действительно определен однозначно для *коммутативных* колец.

Теорема. *Если кольцо R коммутативно, то*

$$R^m \cong R^n \quad \Longleftrightarrow \quad m = n.$$

Доказательство. Пусть $\mathfrak{m}$ — какой-то максимальный идеал кольца R. Тогда фактор-кольцо $K = R/\mathfrak{m}$ является полем. Если, $R^m \cong R^n$, то

$$K^m = (R/\mathfrak{m})^m \cong (R/\mathfrak{m})^n = K^n,$$

и в силу единственности размерности $m = n$.

Эта теорема показывает, что для свободного модуля V над коммутативным кольцом R мы можем без всякой двусмысленности пользоваться обозначением $\mathrm{rk}(V)$. В действительности выполняется даже следующий гораздо более точный факт, который мы не сможем, однако, доказать в общем случае в этой части книги.

Теорема. *Если кольцо R коммутативно, а $U \leq V$ свободные модули, то $\mathrm{rk}(U) \leq \mathrm{rk}(V)$.*

Доказательство для области целостности. Пусть R область целостности, K ее поле частных. Выбрав базис в V мы можем считать, что $V = R^n$, $n = \mathrm{rk}(V)$. Таким образом, $U \leq V = R^n \leq K^n$. Два вектора $u, v \in K^n$ в том и только том случае линейно зависимы над K, когда они линейно зависимы над R. Таким образом, среди элементов U не более n линейно независимых и, значит, любой базис U состоит из $\leq n$ элементов.

Этот результат основан на том, что два любые элемента коммутативного кольца линейно зависимы. В самом деле, если $x, y \in R$, причем хотя бы один из них $\neq 0$, то $xy - yx = 0$. Для некоммутативных колец ничего похожего не имеет места. Так, если $R = K\langle x, y\rangle$ есть кольцо многочленов от двух некоммутирующих переменных x, y над полем K, то $xR + yR$ представляет собой свободный правый подмодуль ранга 2 в свободном правом модуле R_R ранга 1. Это значит, что даже если ранги свободных модулей определены однозначно, СВОБОДНЫЙ МОДУЛЬ МОЖЕТ СОДЕРЖАТЬ ПОДМОДУЛИ СТРОГО БОЛЬШЕГО РАНГА.

§ 6♠. Неединственность ранга

Предположим, что $R^m \cong R^n$ для некоторых $m \neq n$. Это значит, что существуют линейные отображения $\phi : R^m \longrightarrow R^n$ и $\psi : R^n \longrightarrow R^m$ такие, что $\phi\psi = \mathrm{id}_{R^m}$, а $\psi\phi = \mathrm{id}_{R^n}$. Записывая эти линейные отображения как матрицы, мы видим, что над кольцом R существуют неквадратные двусторонне обратимые матрицы. Возможна ли такая ситуация? Большинство учебников линейной алгебры скажут Вам, что нет. Однако в действительности, для некоммутативных колец такая ситуация более, чем возможна. Сейчас мы построим кольцо, над которым $R^2 \cong R$. Итак, мы хотим построить кольцо R и элементы x, y, u, v в нем такие, что

$$(x, y)\begin{pmatrix} u \\ v \end{pmatrix} = xu + yv = 1, \qquad \begin{pmatrix} u \\ v \end{pmatrix}(x, y) = \begin{pmatrix} ux & uy \\ vx & xy \end{pmatrix} = \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix}.$$

Ясно, что над таким кольцом $R^m \cong R^n$ вообще для любых $m, n \in \mathbb{N}$, так что над ним существуют двусторонне обратимые матрицы любого размера!

Теорема. *Существует кольцо R над которым $R^2 \cong R$.*

Доказательство. Пусть K поле, а $R = M_{\mathrm{fc}}(\mathbb{N}, K)$ — кольцо конечно столбцовых матриц. Предъявим элементы x, y, u, v:

$$x = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}, \qquad y = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

$$u = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}, \qquad v = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 1 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Непосредственное вычисление показывает, что $ux = e$, $uy = 0$, $vx = 0$, $vy = e$, и $xu + yv = e$.

Еще раз вдумайтесь в то, что произошло: мы построили пример кольца, над которым все $\neq 0$ свободные правые модули конечного ранга изоморфны между собой.

§ 7♢. Выделение подмодулей уравнениями на координаты

Часто подмодуль свободного модуля удобнее задавать не перечисляя его образующие, а двойственным образом, указывая соотношения, которым удовлетворяют координаты векторов этого подмодуля.

Рассмотрим свободный *правый* модуль $V = R^n$ над кольцом R. Классический способ задания подмодулей в R^n состоит в следующем. Зафиксируем матрицу $a \in M(m, n, R)$ и рассмотрим множество

$$\mathrm{Ker}(a) = \{x \in R^n \mid ax = 0\}.$$

Легко видеть, что $\mathrm{Ker}(a)$ является подмодулем в R^n. В самом деле, $\mathrm{Ker}(a)$ непусто, так как $0 \in \mathrm{Ker}(a)$. При этом, если $x, y \in \mathrm{Ker}(a)$, то $a(x + y) = ax + ay = 0$ и $a(x\lambda) = (ax)\lambda = 0$. Укажем две основные метафоры, связанные с $\mathrm{Ker}(a)$. Эти метафоры особенно часто используются в случае, когда $R = K$ — поле. Дело в том, что в этом случае каждое подпространство в V получается таким способом, так что

Традиционно вычисление $\mathrm{Ker}(a)$ называется **решением системы однородных линейных уравнений**. А именно, если $a = (a_{ij})$ и $x =$

$(x_1, \dots, x_n)^T$, то равенство $ax = 0$ обычно записывается в виде

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0 \\ \quad \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0 \end{cases}$$

и истолковывается как система уравнений относительно $x_1, \dots, x_n$.

• Взяв в качестве матрицы a стандартную строку

$$f_i = (0, \dots, 0, 1, 0, \dots, 0),$$

где 1 стоит на i-м месте, мы получаем подмодуль $\mathrm{Ker}(f_i)$ в R^n, который называется **i-й координатной гиперплоскостью**. Этот подмодуль состоит из всех столбцов $x \in R^n$, для которых $x_i = 0$.

• С другой стороны, взяв в качестве a матрицу $(f_1, \dots, \widehat{f_i}, \dots, f_n)^T$, т.е. единичную матрицу с выброшенной i-й строкой, мы получим подмодуль $\mathrm{Ker}(a)$, состоящий из всех столбцов $x \in R^n$, для которых $x_j = 0$ при всех $j \neq i$. Этот подмодуль называется **i-й координатной осью**.

• Обобщая два предыдущих примера, возьмем теперь произвольное подмножество $I \subseteq \underline{n}$, и положим $a = (f_i)^T$, где $i \in I$. Заметим, что порядок строк здесь не имеет никакого значения, так как он не влияет на $\mathrm{Ker}(a)$. Авторы элементарных учебников имеют обыкновение располагать строки в порядке возрастания индексов: $a = (f_{i_1}, \dots, f_{i_m})^T$, где $I = \{i_1, \dots, i_m\}$, $i_1 < \ldots < i_m$. Подмодуль $\mathrm{Ker}(a)$ называется **координатным подмодулем** в R^n. Этот термин особенно часто используется в случае, когда $R = K$ поле, при этом говорят о **координатных подпространствах**. Координатные гиперплоскости получаются в случае $I = \{i\}$, а координатные оси — в случае $I = \underline{n} \setminus \{i\}$.

• Взяв $a = (1, \dots, 1)$, мы выделим подмодуль $\mathrm{Ker}(a)$, состоящий из всех $x \in R^n$, для которых $x_1 + \ldots + x_n = 0$.

С другой стороны, в теории кодирования подпространство $U = \mathrm{Ker}(a)$ называется **линейным кодом**, а матрица a — **проверочной матрицей** этого линейного кода. В § ? мы узнаем еще один способ задания подпространства U посредством его порождающей матрицы.

§ 8 ♠. Стабильно свободные модули

Модуль P называется **стабильно свободным** ранга $n - m$, если

$$P \oplus R^m = R^n.$$

По определению стабильно свободный модуль — это в точности ядро сюръективного линейного отображения

$$R^n \mapsto R^m, \qquad x \mapsto ax,$$

где $a \in M(m, n, R)$ матрица, столбцы которой порождают R^m.

Теорема. *Над коммутативным кольцом R каждый стабильно свободный модуль ранга 1 свободен.*

Эта теорема не обобщается ни на некоммутативный случай, ни на модули ранга ≥ 2 над коммутативным кольцом.

Пример 1. Вот простой пример стабильно свободного, но не свободного модуля ранга 2. Пусть

$$R = \mathbb{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$$

кольцо полиномиальных функций на сфере $\mathbb{S}^2$. Модуль

$$P = \left\{ \begin{pmatrix} f \\ g \\ h \end{pmatrix} \;\middle|\; f, g, h \in R,\ xf + yg + zh = 0 \right\} \leq R^3$$

касательных векторных полей к $\mathbb{S}^2$ стабильно свободен. Однако, как хорошо известно, этот модуль не может быть свободным: на $\mathbb{S}^2$ не существует двух касательных векторных полей, которые были бы линейно независимы в каждой точке.

Пример 2. А вот простой пример стабильно свободного модуля ранга 1 над кольцом $D[x, y]$ многочленов от двух (коммутирующих) переменных над телом D, построенный Оянгуреном и Сридхараном. Пусть $\alpha, \beta \in D$ таковы, что $\alpha\beta \neq \beta\alpha$. Тогда модуль

$$P = \left\{ \begin{pmatrix} f \\ g \end{pmatrix} \;\middle|\; f, g \in D[x, y],\ (x + \alpha)f + (y + \beta)g = 0 \right\} \leq R^2$$

стабильно свободен, но не свободен. В то же время замечательная теорема Суслина утверждает, что любой стабильно свободный модуль ранга ≥ 2 над кольцом многочленов $D[x_1, \dots, x_n]$ свободен.

§ 9 $\diamondsuit$. Матрица перехода от базиса к базису

1. Матрица перехода. Пусть V — свободный правый модуль над R, $u_1, \dots, u_n$ — базис V, а $v_1, \dots, v_m$ — произвольные векторы в V. Разложим каждый из векторов v_i по базису $u_1, \dots, u_n$:

$$v_j = \sum_{i=1}^{n} u_i a_{ij}, \qquad 1 \leq j \leq m.$$

При этом j-м столбцом матрицы $a = (a_{ij}) \in M(m, n, R)$ является столбец координат вектора v_j в базисе $u_1, \dots, u_n$. В наиболее важном случае, когда $v_1, \dots, v_m$ тоже является базисом V, получающаяся так матрица a называется **матрицей перехода** от базиса $u_1, \dots, u_n$ к базису $v_1, \dots, v_m$. Часто для краткости базисы записываются одной буквой, в этом случае об a говорят как о матрице переходе от базиса u к базису v. При этом u называется **старым базисом**, а v — **новым базисом**.

Предостережение. В большинстве элементарных учебников линейной алгебры, авторы которых не в состоянии отличить правое от левого, матрица перехода задается следующей бесстыдной формулой, $v_j = \sum a_{ij} u_i$.

Чтобы не вводить каждый раз специальную букву, мы будем обозначать матрицу перехода от базиса $u_1, \ldots, u_n$ к базису $v_1, \ldots, v_m$ через $(u \rightsquigarrow v)$. Определение матрицы перехода короче и нагляднее выражается в следующей форме

$$(v_1, \ldots, v_m) = (u_1, \ldots, u_m)(u \rightsquigarrow v),$$

именно в такой форме мы обычно и будем им пользоваться.

Теорема. *Матрица перехода обладает следующими свойствами.*

- $(u \rightsquigarrow u) = e;$
- $(u \rightsquigarrow v)(v \rightsquigarrow w) = (u \rightsquigarrow w);$
- $(u \rightsquigarrow v)(v \rightsquigarrow u) = e.$

Доказательство. Первое свойство очевидно, оно означает в точности, что $u_i = u_i$. Второе свойство доказывается непосредственным вычислением. А именно, пусть $w_1, \ldots, w_l$ — третий базис модуля V, тогда

$$\begin{aligned}(u_1, \ldots, u_n)(u \rightsquigarrow w) = (w_1, \ldots, w_l) = \\ (v_1, \ldots, v_m)(u \rightsquigarrow u) = (u_1, \ldots, u_n)(u \rightsquigarrow v)(v \rightsquigarrow w).\end{aligned}$$

Наконец, третье свойство сразу следует из первого и второго.

В силу симметрии между u и v третье свойство может быть переписано в виде $(u \rightsquigarrow v)^{-1} = (v \rightsquigarrow u)$. Таким образом, из этой теоремы вытекает такое довольно неожиданное следствие: если в свободном модуле над кольцом существуют базисы, состоящие из разного количества элементов, то над таким кольцом существуют неквадратные двусторонне обратимые матрицы. В следующем параграфе мы убедимся, что кольца, для которых подобная неприятность случается, действительно существуют.

§ 10 ♢. Преобразование координат

Там, где было **оно**, должно быть **я**.

Зигмунд Фрейд

Рассмотрим выражение одного и того же вектора $z \in V$ в двух базисах $u_1, \ldots, u_n$ и $v_1, \ldots, v_m$:

$$z = (u_1, \ldots, u_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (v_1, \ldots, v_m) \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}.$$

Как связаны между собой координаты вектора z в базисе u — **старые координаты** — с его **новыми координатами**, т. е. координатами в базисе v? Проведем обычное вычисление, сравнив разложения z по двум базисам и перейдя в разложении по старому базису к новому:

$$(v_1,\dots,v_m)\begin{pmatrix} y_1\\ \vdots\\ y_m\end{pmatrix} = z = (u_1,\dots,u_n)\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix} =$$

$$(u_1,\dots,u_n)(u\rightsquigarrow v)(u\rightsquigarrow v)^{-1}\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix} =$$

$$(v_1,\dots,v_m)(u\rightsquigarrow v)^{-1}\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}.$$

Здесь как и в предыдущем параграфе через $(u\rightsquigarrow v)\in M(m,n,R)$ обозначена матрица перехода от старого базиса u к новому базису v.

В силу единственности координат мы видим

$$\begin{pmatrix} y_1\\ \vdots\\ y_m\end{pmatrix} = (u\rightsquigarrow v)^{-1}\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix},$$

или, что то же самое,

$$\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix} = (u\rightsquigarrow v)\begin{pmatrix} y_1\\ \vdots\\ y_m\end{pmatrix}.$$

Эти формулы весьма поучительны, они показывают, что новые координаты получаются из старых координат вовсе не умножением на матрицу перехода от старого базиса к новому, а умножением на обратную к ней. Иными словами, координаты преобразуются в направлении противоположном преобразованию базисов! Эту мысль обычно выражают говоря, что координаты преобразуются **контравариантно** по отношению к изменению базиса. В действительности, большинство геометрических объектов, с которыми мы будем иметь дело в этой книге, являются **тензорами**, иными словами, они преобразуются либо **ковариантно**, т. е. при помощи матрицы перехода от старого базиса к новому, либо контравариантно, т. е. при помощи матрицы перехода от нового базиса к старому, либо, в общем случае, ковариантно по одним индексам и контравариантно по другим.

§ 11 ♢. Координатные системы в проективных модулях

Для того, чтобы провести большинство классических рассуждений линейной алгебры, совершенно несущественно, что в модуле M существует базис. Однако все они опираются на то, что в модуле существуют координатные функции $\phi_i \in M^*$ по отношению к этому базису. Но в действительности координаты можно ввести и в том случае, когда базиса нет.

Определение. *Говорят, что* (x_i, ϕ_i), $i \in I$ *является* **координатной системой** *модуля* M, *если*

- $x_i \in M$, $i \in I$, *— система образующих модуля* M*;*
- $\phi_i \in M^*$, *причем для каждого* $x \in M$ *только конечное число* $\phi_i(x)$ *отлично от 0;*
- *любой элемент* $x \in M$ *представляется в виде*

$$x = \sum_{i \in I} \phi_i(x) x_i.$$

Значение $\phi_i(x) \in R$ *называется* ***i*-й координатой** *вектора* $x \in M$ *по отношению к этой координатной системе.*

Предостережение. Разумеется, если векторы x_i, $i \in I$, не являются линейно независимыми, то вектор $x \in M$ допускает и другие выражения в качестве линейных комбинаций векторов x_i, $i \in I$, кроме выражения $x = \sum \phi_i(x) x_i$. Однако это обычно ни на что не влияет. Для каждого вектора x координатная система *выбирает* единственное выражение x в качестве линейной комбинации x_i, $i \in I$, причем делает это *согласованным образом*, т.е. так, что все координатные функции линейно зависят от x. В большинстве классических рассуждений только это и используется.

Понятие координатной системы является обобщением понятия базиса. Мы знаем, что модуль в том и только том случае свободен, когда в нем существует базис. Оказывается, проективные модули допускают аналогичную характеризацию в терминах координатных систем.

Теорема. *Модуль* P *в том и только том случае проективен, когда в нем существует координатная система.*

Доказательство. Предположим вначале, что P проективен. Найдется свободный модуль F с базисом y_i, $i \in I$, и эпиморфизм $\psi : F \longrightarrow P$. Тогда элементы $x_i = \phi(y_i)$ порождают P. В силу проективности модуля P эпиморфизм ψ допускает сечение $\theta : P \longrightarrow F$, $\psi \circ \theta = \mathrm{id}_P$, и, значит, $\theta(P)$ выделяется прямым слагаемым в F. Для любого $x \in P$ элемент $\theta(x)$ представляется в виде $\theta(x) = \sum \phi_i(x) y_i$, где только конечное число $\phi_i(x) \in R$ отлично от нуля. Непосредственно из определения ясно, что $\phi_i \in P^*$ (впрочем, в этом можно убедиться и так: ϕ_i является композицией θ и проекции F на слагаемое $Rx_i \cong R$). Применив ϕ к обеим частям этого равенства, мы как раз и получим равенство $x = \sum \phi_i(x) x_i$.

Обратно, предположим, что в модуле P существует координатная система (x_i, ϕ_i), $i \in I$. Рассмотрим свободный модуль F с базисом y_i, $i \in I$, и определим гомоморфизм $\psi : F \longrightarrow P$ такой, что $\psi(y_i) = x_i$. Полагая

$\theta(x) = \sum \phi_i(x) y_i$ для каждого $x \in P$, мы получим сечение этого эпиморфизма. Таким образом, $\theta(P) \cong P$ является прямым слагаемым F и, значит, модуль P проективен.

Глава 3. ВЕКТОРНЫЕ ПРОСТРАНСТВА

Жить в эпоху свершений, имея возвышенный нрав,
к сожалению, трудно.

Иосиф Бродский, *Конец прекрасной эпохи*

В настоящей главе мы продолжаем сужать предмет нашего изучения. А именно, мы переходим к изучению векторных пространств над полями. Каждое векторное пространство является свободным модулем. Однако, в действительности специфика поля *гораздо* глубже и состоит не в существовании базисов как таковом, а в существовании *относительных* базисов. Иными словами, в том, что каждый подмодуль векторного пространства выделяется в нем прямым слагаемым — или, что то же самое, в том, что каждая линейно независимая система векторов может быть включена в некоторый базис. Для свободных модулей над кольцами, не являющимися полями, это безнадежно неверно! Таким образом, в отличие от модулей векторные пространства над полем не имеют вообще никакой арифметики, только геометрию. Иными словами, большая часть общих результатов о векторных пространствах вообще не зависит от поля.

§ 1$\diamondsuit$. Линейная зависимость над полем

Отметим, прежде всего, важнейшую переформулировку условия линейной зависимости, в которой явным образом используется тот факт, что K поле.

Предложение. *Пусть V векторное пространство над полем. Векторы $u_1,\dots,u_n \in V$ в том и только том случае линейно зависимы, когда один из них является линейной комбинацией остальных.*

Доказательство. ($\Longleftarrow$) Предположим, что один из векторов u_i является линейной комбинацией остальных. Пусть, например, u_j есть линейная комбинация u_i, $i \neq j$, т.е. $u_j = \sum u_i\lambda_i$, $i \neq j$. Полагая $\lambda_j = -1$, получим $u_1\lambda_1 + \ldots + u_n\lambda_n = 0$, причем эта линейная зависимость нетривиальна, так как $\lambda_j \neq 0$.

($\Longrightarrow$) Обратно, пусть $u_1,\dots,u_n$ линейно зависимы и $u_1\lambda_1+\ldots+u_n\lambda_n = 0$ — нетривиальная линейная зависимость между ними. Тогда хотя бы один коэффициент этой зависимости отличен от 0, скажем, $\lambda_j \neq 0$. Разделив эту зависимость на λ_j и перенеся все члены, кроме j-го, в другую часть, получим $u_j = -\sum u_i\lambda_i$, где сумма берется по всем $i \neq j$.

Замечание. Ключевым моментом в доказательстве предложения является возможность разделить на λ_j. В случае, когда кольцо коэффициентов R

модуля M не является полем, это совершенно не так. Дело в том, что в любые два элемента $x, y \in R$ *коммутативного* кольца R, рассматриваемого как модуль над собой, линейно зависимы в нем: $yx + (-x)y = 0$. В то же время, конечно, ниоткуда не следует, что один из них должен быть кратным другого:

• $2, 3 \in \mathbb{Z}$ линейно зависимы над $\mathbb{Z}$, но ни один из них не является целочисленным кратным второго.

• $x, y \in K[x, y]$ линейно зависимы над $K[x, y]$, но ни один из них не является полиномиальным кратным второго.

В действительности, для других модулей дела обстоят еще значительно хуже:

• Рассмотрим $M = \mathbb{Z}/m\mathbb{Z}$ как модуль над $\mathbb{Z}$. Тогда система, состоящая из *одного* вектора $u = \overline{1} \in M$, будет линейно зависимой, хотя $u \neq 0$.

Из предложения вытекает, что для векторных пространств над полем такое невозможно: система, состоящая из одного ненулевого вектора *всегда* линейно независима.

Мы будем часто использовать проведенное в доказательстве предложения рассуждение в следующей форме. А именно, предложение можно было бы сформулировать в следующей более точной форме: *то* из u_i, которое входит в линейную зависимость между ними с ненулевым коэффициентом, является линейной комбинацией остальных.

Следствие. *Если векторы $u_1, \ldots, u_n$ линейно независимы, а*

$$x \notin \langle u_1, \ldots, u_n \rangle,$$

то $u_1, \ldots, u_n, x$ тоже линейно независимы.

Доказательство. Пусть $u_1\lambda_1 + \ldots + u_n\lambda_n + x\mu = 0$ линейное соотношение между $u_1, \ldots, u_n, x$. Как мы только что заметили, если $\mu \neq 0$, то x является линейной комбинацией $u_1, \ldots, u_n$. С другой стороны, если $\mu = 0$, то $u_1, \ldots, u_n$ линейно зависимы. И то и другое невозможно.

Обычно мы будем использовать обратное утверждение.

Следствие. *Если векторы $u_1, \ldots, u_n$ линейно независимы, а $u_1, \ldots, u_n, x$ линейно зависимы, то*

$$x \in \langle u_1, \ldots, u_n \rangle.$$

В действительности это предложение можно несколько уточнить, проследив, какой именно из векторов u_i входит с ненудевым коэффициентом.

Условие замены Штейница. *Пусть V векторное пространство над полем, $u_1, \ldots, u_{n-1}, v, w \in V$. Предположим, что*

$$v \in \langle u_1, \ldots, u_{n-1}, w \rangle, \qquad v \notin \langle u_1, \ldots, u_{n-1} \rangle,$$

тогда $w \in \langle u_1, \dots, u_{n-1}, v\rangle$.

Доказательство. Пусть

$$v = u_1\lambda_1 + \ldots + u_{n-1}\lambda_{n-1} + w\mu.$$

Так как u не является линейной комбинацией $u_1, \dots, u_{n-1}$, то $\mu \neq 0$. Разделив на μ и перенося в другую часть, мы видим, что

$$w = v\mu^{-1} - u_1\lambda_1\mu^{-1} - \ldots - u_{n-1}\lambda_{n-1}\mu^{-1}.$$

§ 2◇. Теорема Штейница: доказательство методом замены

Важнейшая связь между понятиями линейных комбинаций и линейной зависимости описывается следующей теоремой, которая позволит нам в дальнейшем охарактеризовать векторные пространства их размерностями. Эта теорема утверждает, что среди линейных комбинаций какого-то семейства векторов не может быть больше линейно независимых, чем среди исходных векторов. Этот факт, называемый также **теоремой о линейной зависимости линейных комбинаций**, справедлив для любых коммутативных колец.

Теорема Штейница. *Пусть* V *— модуль над коммутативным кольцом* R, $v_1, \dots, v_n \in V$ *и*

$$u_1, \dots, u_m \in \langle v_1, \dots, v_n\rangle,$$

причем $m > n$. *Тогда* $u_1, \dots, u_m$ *линейно зависимы.*

К сожалению, сейчас мы сможем доказать этот результат только для случая, когда $R = K$ поле. Конечно, если теорема верна для полей, она верна также для областей целостности. Однако, для произвольных коммутативных колец ни метод замены, ни метод исключения не работают. Все обычные доказательства для колец с делителями нуля используют чуть более патетические средства такие, как, скажем, теорема Гильберта о базисе, метод Кронекера, теория определителей или что-нибудь в таком духе. Кроме того, конечно, сформулированная ниже более сильная форма теоремы Штейница не имеет места даже для кольца $\mathbb{Z}$. Разумеется, специфика поля определяется вовсе не тем, что среди элементов $u_1, \dots, u_m$ не более n линейно независимых, а именно возможностью заменять v_i на u_j.

Доказательство методом замены. Индукция по n.

База индукции. Пусть $u_1 = v_1\lambda_1$ и $u_2 = v_1\lambda_2$. Если $\lambda_1 = 0$, то доказывать нечего, так как в этом случае система $\{0, u_2\}$ линейно зависима. В противном случае, когда $\lambda_1 \neq 0$, равенство $u_1\lambda_2 - u_2\lambda_1 = 0$ есть нетривиальная линейная зависимость между u_1 и u_2.

Шаг индукции. Пусть $u_1, \dots, u_m \in \langle v_1, \dots, v_n \rangle$. Если $u_1, \dots, u_m \in \langle v_2, \dots, v_n \rangle$, то в действительности $u_1, \dots, u_m$ являются линейными комбинациями не n а уже $n-1$ вектора и, значит, мы можем применить индукционное предположение.

С другой стороны, если $u_1, \dots, u_m \notin \langle v_2, \dots, v_n \rangle$, то существует u_i, допустим, u_1, в разложение которого фактически входит v_1. Тогда по условию замены $v_1 \in \langle u_1, v_2, \dots, v_n \rangle$ и, тем самым, $u_2, \dots, u_m \in \langle u_1, v_2, \dots, v_n \rangle$.

Теперь мы можем повторить то же самое рассуждение для v_2 вместо v_1. В самом деле, если $u_2, \dots, u_m \in \langle u_1, v_3, \dots, v_n \rangle$, то мы снова можем применить индукционное предположение. Поэтому существует u_i, допустим, u_2, не принадлежащее $\langle u_1, v_3, \dots, v_n \rangle$. По условию замены $v_2 \in \langle u_1, u_2, v_3, \dots, v_n \rangle$ и, значит, $u_3, \dots, u_m \in \langle u_1, u_2, v_3, \dots, v_n \rangle$.

Продолжая действовать таким образом, мы либо сможем применить индукционное предположение, либо докажем, что $u_{n+1}, \dots, u_m \in \langle u_1, \dots, u_n \rangle$. Но это и значит, что между u_i существует нетрививальная линейная зависимость.

В действительности, это доказательство доказывает значительно больше, чем утверждалось.

Теорема Штейница. *Если $u_1, \dots, u_m \in \langle v_1, \dots, v_n \rangle$ линейно независимы, то $m \leq n$ и, возможно после перенумерации u_i,*

$$\langle u_1, \dots, u_m, v_{m+1}, \dots, v_n \rangle = \langle v_1, \dots, v_n \rangle.$$

§ 3♢. Теорема Штейница: доказательство методом исключения

Comment on faisait l'amour sous l'ancien régime.

Charles Baudelaire

В этом параграфе мы ввиду ключевой важности теоремы Штейница для линейной алгебры над полем, приведем еще одно ее доказательство. Это как раз то доказательство, которое традиционно используется для фактического вычисления ранга.

Доказательство методом исключения. Ясно, что можно без потери общности считать, что $m = n+1$. Будем вести доказательство индукцией по n. Так как база уже имеется, то достаточно провести шаг индукции.

Шаг индукции. Предположим, что теорема уже доказана для $n-1$. Докажем ее для n. Пусть

$$\begin{aligned} u_1 &= v_1\lambda_{11} + \dots + v_n\lambda_{1n} \\ &\dots\dots\dots\dots\dots\dots \\ u_m &= v_1\lambda_{m1} + \dots + v_n\lambda_{mn} \end{aligned}$$

выражения для $u_1, \dots, u_m$ в качестве линейных комбинаций $v_1, \dots, v_n$.

Если при этом все коэффициенты $\lambda_{1n}, \dots, \lambda_{mn}$ равны 0, то в действительности векторы $u_1, \dots, u_m$ являются линейными кобинациями уже векторов $v_1, \dots, v_{n-1}$, в количестве $(n-1)$ штуки. Это значит, что мы можем применить индукционное предположение и заключить, что $u_1, \dots, u_m$ линейно зависимы.

Пусть, поэтому, хотя бы один из коэффициентов $\lambda_{1n}, \dots, \lambda_{mn}$ отличен от 0. Перенумеровывая, если нужно, $u_1, \dots, u_m$, можно считать, что $\lambda_{mn} \neq 0$. В этом случае рассмотрим векторы

$$w_i = u_i - u_m \lambda_{in} \lambda_{mn}^{-1}, \qquad i = 1, \dots, m-1.$$

Коэффициент $-\lambda_{in}\lambda_{mn}^{-1}$ подобран с таким расчетом, чтобы члены, содержащие v_n, в выражениях для u_i и u_m в качестве линейной комбинации $v_1, \dots, v_n$ взаимно сократились.

Это значит, что в действительности векторы $w_1, \dots, w_{m-1}$ являются линейными комбинациями уже $n-1$ штук векторов $v_1, \dots, v_{n-1}$. Так как $m > n$, то $m-1 > n-1$ и, следовательно, мы можем применить индукционное предположение и заключить, что векторы $w_1, \dots, w_{m-1}$ линейно зависимы. Пусть, например,

$$w_1\mu_1 + \ldots + w_{m-1}\mu_{m-1} = 0$$

является нетривиальной линейной зависимостью между ними, т. е. не все μ_i здесь равны 0. Подставляя в эту зависимость выражения для w_i через u_i, получаем

$$(u_1 - u_m\lambda_{1n}\lambda_{mn}^{-1})\mu_1 + \ldots + (u_i - u_m\lambda_{m-1,n}\lambda_{mn}^{-1})\mu_{m-1} =$$

$$u_1\mu_1 + \ldots + u_{m-1}\mu_{m-1} - u_m(\lambda_{1n}\lambda_{mn}^{-1}\mu_1 + \ldots + \lambda_{m-1,n}\lambda_{mn}^{-1}\mu_{m-1}) = 0,$$

что представляет собой нетривиальную линейную зависимость между векторами $u_1, \dots, u_m$, так как уже не все μ_i равны 0.

§ 4◊. Минимальные порождающие системы

В этом и следующем параграфах мы дадим еще две эквивалентные формулировки понятия базиса. Напомним, что порождающая система называется минимальной, если любая ее собственная подсистема уже не порождает V. Иными словами, она является минимальным элементом в множестве всех порождающих систем относительно порядка, заданного включением.

Теорема. *Для системы векторов $v_1, \dots, v_n$ следующие условия эквивалентны:*

(1) $v_1, \dots, v_n$ — *базис,*

(3) $v_1, \dots, v_n$ — *минимальная порождающая система.*

Доказательство. (1) $\Longrightarrow$ (3) Пусть $v_1, \dots, v_n$ — базис пространства V. По определению $v_1, \dots, v_n$ является порождающей системой. Проверим, что в действительности это минимальная порождающая система. Предположим, что это не так. Тогда выбросив некоторый вектор v_j мы снова получаем порождающую систему, так что, в частности, v_j является линейной комбинацией остальных векторов v_i, $i \neq j$. Тем самым, по предложению из пункта 3 векторы v_i линейно зависимы.

(3) $\Longrightarrow$ (1) Пусть $v_1, \dots, v_n$ — минимальная порождающая система. Предположим, что она не является базисом. Это может произойти только за счет того, что векторы $v_1, \dots, v_n$ линейно зависимы. В этом случае по предложению из пункта 3 один из векторов, скажем, v_j является линейной комбинацией остальных, т.е. $v_j \in \langle v_1 \dots, \widehat{v_j}, \dots, v_n \rangle$, где крышка над j-м вектором означает, что он должен быть опущен. Таким образом,

$$\langle v_1 \dots, \widehat{v_j}, \dots, v_n \rangle = \langle v_1 \dots, v_n \rangle = V,$$

что противоречит минимальности $v_1, \dots, v_n$.

Эта теорема позволяет доказать существование базиса.

Теорема. *Из любой порождающей системы векторов может быть извлечен базис.*

Доказательство для конечномерного случая. Выберем в м какую-то порождающую систему: $V = \langle v_1, \dots v_n \rangle$. Тогда, если $v_1, \dots, v_n$ не является базисом, то про предыдущей теореме она не минимальна, т.е. какой-то из этих векторов является линейной комбинацией остальных. Переставляя, если нужно, векторы v_i, можно считать, что $v_n \in \langle v_1, \dots v_{n-1} \rangle$, таким образом, $V = \langle v_1, \dots v_{n-1} \rangle$. Применив теперь то же рассуждение к системе $v_1, \dots, v_{n-1}$, мы видим, что либо она является базисом, либо какой-то из векторов v_i можно исключить, получив меньшую порождающую систему. Этот процесс обрывается на конечном шаге и последняя получающаяся порождающая система обязана быть базисом.

Теорема продолжает оставаться верной и для бесконечномерного случая, но здесь ее доказательство перестает быть конструктивным, из-за необходимости использовать лемму Куратовского—Цорна.

Доказательство для общего случая. Пусть Ω — множество всех порождающих систем векторов, содержащихся в данной системе. Тогда инфимум убывающей цепи элементов Ω снова принадлежит Ω, поэтому в Ω существуют минимальные элементы.

Это доказательство, разумеется, ничего не говорит о том, как именно построить такой минимальный элемент — оно в явном виде использует аксиому выбора.

§ 5$\diamondsuit$. Максимальные линейно независимые системы

Сейчас мы дадим описание базисов, двойственное к полученному в предыдущем параграфе. Напомним, что линейно независимая система называется максимальной, если любая ее собственная надсистема уже не является линейно независимой. Иными словами, эта система максимальна в множестве всех линейно независимых систем, упорядоченных по включению.

Теорема. *Для системы векторов $v_1, \dots, v_n \in V$ следующие условия эквивалентны:*

(1) $v_1, \dots, v_n$ — *базис,*

(4) $v_1, \dots, v_n$ — *максимальная линейно независимая система.*

Доказательство. (1) $\Longrightarrow$ (4). Пусть $v_1, \dots, v_n$ — базис пространства V. По определению $v_1, \dots, v_n$ линейно независимы. Проверим, что в действительности это максимальная линейно независимая система. Предположим, что это не так. Тогда добавив некоторый вектор v мы снова получим линейно независимую систему, так что, в частности, v не является линейной комбинацией остальных векторов $v_1, \dots, v_n$. Тем самым, $v_1, \dots, v_n$ не является порождающей системой, что противоречит определению базиса.

(4) $\Longrightarrow$ (1). Пусть $v_1, \dots, v_n$ — максимальная линейно независимая система. Предположим, что она не является базисом. Это может произойти только за счет того, что векторы $v_1, \dots, v_n$ не порождают пространство V. В этом случае найдется вектор v, который не является линейной комбинацией векторов $v_1, \dots, v_n$. Мы утверждаем, что получающаяся система $v_1, \dots, v_n, v$, состоящая из $n+1$ вектора, линейно независима. В самом деле, пусть

$$v_1\lambda_1 + \ldots + v_n\lambda_n + v\lambda = 0$$

нетривиальная линейная зависимость между этими векторами. Тогда $\lambda = 0$ — иначе v был бы линейной комбинацией векторов $v_1, \dots, v_n$. Значит, исходные векторы не являются линейно независимыми. Это значит, что система $v_1, \dots, v_n, v$ линейно независима, что противоречит максимальности $v_1, \dots, v_n$.

Эта теорема позволяет дать другое доказательство существования базиса.

Теорема. *Любая линейно независимая системя векторов может быть дополнена до базиса.*

Доказательство для конечномерного случая. Выберем в V какую-то линейно независимую систему $v_1, \dots, v_n$. Если $v_1, \dots, v_n$ не является базисом, то про предыдущей теореме она не максимальна, т.е. найдется вектор v_{n+1}, не являющийся линейной комбинацией $v_1, \dots, v_n$. В этом случае система $v_1, \dots, v_{n+1}$ линейно независима, и, применив к ней то же рассуждение, мы видим, что либо она является базисом, либо можно найти вектор v_{n+2}, не являющийся линейной комбинацией векторов этой системы, получив большую линейной независимую систему. Так как пространство V конечномерно, то (по теореме о линейной зависимости линейных комбинаций) этот процесс обрывается на конечном шаге и последняя получающаяся линейно независимая система обязана быть базисом.

Сюда применимо то же рассуждение, что и в конце предыдущего параграфа. Теорема продолжает оставаться верной и для бесконечномерного случая, но здесь ее доказательство перестает быть конструктивным.

Доказательство для общего случая. Пусть Ω — множество всех линейно независимых систем векторов, содержащих данную систему. Тогда супремум возрастающей цепи элементов Ω снова принадлежит Ω, поэтому по лемме Куратовского—Цорна в Ω существуют максимальные элементы.

Также и это доказательство ничего не говорит о том, как именно построить такой максимальный элемент.

Задача. Докажите, что если $X \subseteq Y$ два подмножества в V, причем X линейно независимо, а Y является системой образующих V, то существует базис Z пространства V такой, что $X \subseteq Z \subseteq Y$.

§ 6$\diamondsuit$. Существование базисов

Резюмируем доказанное в главе 2 и двух предшествующих параграфах.

Теорема. *Для системы векторов $v_1, \dots, v_n \in V$ следующие условия эквивалентны:*

(1) $v_1, \dots, v_n$ — *базис;*

(2) *каждый вектор $v \in V$, единственным образом представляется в виде линейной комбинации $v_1, \dots, v_n$;*

(3) $v_1, \dots, v_n$ — *минимальная порождающая система;*

(4) $v_1, \dots, v_n$ — *максимальная линейно независимая система.*

Заметим теперь, что из результатов двух предыдущих пунктов сразу вытекает, что в любом векторном пространстве над полем K существует базис.

Теорема. *В любом векторном пространстве V над полем K существует базис, причем любые два базиса пространства V равномощны.*

Доказательство для конечномерного случая. Докажем вначале существование. Так как пространство V конечномерно, в нем существует конечная порождающая система $v_1, \dots, v_n$. Согласно пункту 6 из нее может быть извлечен базис. можно доказать существование базисов и иначе, опираясь на результаты пункта 7. Пустая система векторов пространства м линейно независима и, следовательно, может быть дополнена до базиса.

Докажем теперь равномощность любых двух базисов. В самом деле, пусть $u_1, \dots, u_m$ и $v_1, \dots, v_n$ — два базиса векторного пространства V. Тогда векторы $u_1, \dots, u_m$ являются линейными комбинациями векторов $v_1, \dots, v_n$ и по теореме о линейной зависимости линейных комбинаций, число линейно независимых среди них не превосходит n, т.е. так как $u_1, \dots, u_m$ линейно независимы, $m \leq n$. Так как $u_1, \dots, u_m$ и $v_1, \dots, v_n$ входят сюда совершенно симметрично, по той же причине $n \leq m$.

Замечание. Теорема продолжает оставаться верной и для бесконечномерного случая, но, как уже отмечалось, ее доказательство опирается на трансфинитную индукцию и не является конструктивным. Например, известно, что в $\mathbb{R}$ существует базис как у векторного пространства над $\mathbb{Q}$, но ни одного такого базиса построить нельзя. В действительности, бесконечномерные пространства обычно несут на себе какую-то дополнительную структуру (топологию, метрику и т.д.) и в этом случае рассматривается другое понятие базиса, отличающееся от рассматриваемого нами.

§ 7♢. Размерность векторного пространства

Сейчас мы введем важнейший инвариант векторных пространств.

Определение. *Общая мощность всех базисов пространства м называется* **размерностью** *пространства V над K и обозначается* $\dim_K(V)$ *или, если поле K фиксировано, просто* $\dim(V)$.

Приведем несколько примеров.

• Размерность нулевого пространства равна 0 — его базисом является пустое множество. Размерность прямой равна 1 — базисом является система, состоящая из любого ненулевого вектора. Размерность плоскости равна 2 — базис состоит из двух любых неколлинеарных векторов. Размерность трехмерного пространства (как ясно из названия) равна 3 — базисом является любая тройка некомпланарных векторов.

• Вообще, $\dim(K^n) = n$ и $\dim({}^nK) = n$.

• Комплексные числа двумерны над вещественными: $\dim_{\mathbb{R}}(\mathbb{C}) = 2$, а кватернионы — четырехмерны $\dim_{\mathbb{R}}(\mathbb{H}) = 4$. С другой стороны, $\dim_{\mathbb{C}}(\mathbb{C}) = 1$ и $\dim_{\mathbb{C}}(\mathbb{H}) = 2$.

• Кольцо многочленов $K[x]$, рассматриваемое как векторное пространство над K, бесконечномерно. В действительности, в этом случае размерность счетна, $\dim_K(K[x]) = \aleph_0$.

• Кольцо многочленов Лорана $K[x, x^{-1}]$, рассматриваемое как векторное пространство над K, бесконечномерно. В этом случае размерность по-прежнему счетна, $\dim_K(K[x, x^{-1}]) = \aleph_0$.

• Кольцо рациональных дробей $K(x)$, рассматриваемое как векторное пространство над K, бесконечномерно. В действительности, из основной теоремы о рациональных дробях (разложение правильной дроби на простейшие) следует, что если K конечно, то размерность счетна, $\dim_K(K(x)) = \aleph_0$, но если K бесконечно, то $\dim_K(K(x)) = |K|$. В частности,

$$\dim_{\mathbb{R}}(\mathbb{R}(x)) = \dim_{\mathbb{C}}(\mathbb{C}(x)) = 2^{\aleph_0}$$

— почему-то большинство начинающих и даже некоторые профессиональные аналисты верят, что $K(x)$ счетномерно!!!

• Вещественные числа бесконечномерны над рациональными, в действительности, в этом случае размерность равна мощности континуума:

$$\dim_{\mathbb{Q}}(\mathbb{R}) = 2^{\aleph_0}.$$

Вскоре мы покажем, что в действительности размерность является единственным инвариантом векторного пространства с точностью до изоморфизма, т.е. что любые два пространства одинаковой размерности изоморфны.

Замечание. Результаты настоящего пункта нарушаются для колец, даже таких просто устроенных колец, как $\mathbb{Z}$. Во-первых, далеко не во всяком R-модуле существует базис. Например, $\mathbb{Z}$-модуль $M = \mathbb{Z}/m\mathbb{Z}$ вообще не имеет базисов: он не равен 0, но любая непустая система векторов в нем линейно зависима. Вообще, модуль в том и только том случае имеет базис, когда он свободен, и теорема настоящего пункта может быть сформулирована в следующей форме: любой модуль над полем свободен. Как мы только что убедились, над $\mathbb{Z}$ существуют модули не являющиеся свободными. Размерность векторного пространства — это в точности то же самое, что в пункте 1 называлось рангом свободного модуля. Из теории определителей будет следовать, что для коммутативного кольца ранг является единственным инвариантом свободного модуля с точностью до изоморфизма. Для некоммутативных колец ситуация может быть еще значительно более сложной. В этом случае даже для свободных (левых или правых) R-модулей ранг не определен однозначно, т.е. существуют кольца R такие, что $R^m \cong R^n$ для некоторых $m \neq n$.

Принцип Дирихле утверждает, что отображение конечного множества в себя в том и только случае биективно, когда оно инъективно, когда оно сюръективно. Следующий результат представляет собой типичную иллюстрацию этого принципа.

Теорема. *Пусть $v_1, \dots, v_n \in V$, где $\dim(V) = n$. Тогда следующие условия эквивалентны:*

- *$v_1, \dots, v_n$ базис V,*
- *$v_1, \dots, v_n$ порождают V,*
- *$v_1, \dots, v_n \in V$ линейно независимы.*

Так как базис подпространства линейно независим, мы получаем такое важное следствие, известное как `Dimensionsargument`.

Следствие. *Если $U \leq V$ и $\dim(V) < \infty$, то*

$$U = V \qquad \Longleftrightarrow \qquad \dim(U) = \dim(V).$$

§ 8♢. Относительный базис, коразмерность

Пусть $U \leq V$ — подпространство правого векторного пространства над K. Векторы $v_a, \dots, v_n \in V$ называются **линейно независимыми** над K **относительно** U, если из того, что

$$v_1\lambda_1 + \ldots + v_n\lambda_n \in U$$

вытекает, что $\lambda_1 = \ldots = \lambda_n = 0$.

Говорят, что $v_a, \dots, v_n \in V$ **порождают** V над K **относительно** U, если

$$V = \langle v_a, \dots, v_n \rangle + U.$$

Говорят, что $v_a, \dots, v_n \in V$ образуют **базис** пространства V **относительно** U, если они линейно независимы относительно U и порождают V относительно U.

Теорема. *Следующие условия эквивалентны.*

- $v_1, \dots, v_n$ *базис* V *относительно* U.
- $v_1 + U, \dots, v_n + U$ — *базис* V/U.
- $v_1, \dots, v_n$ *какого-то базиса* U *до базиса* V.
- $\langle v_1, \dots, v_n \rangle$ — *дополнение* U *в* V, *иными словами,*

$$V = \langle v_1, \dots, v_n \rangle \oplus U.$$

Доказательство.

$$(v_1 + U)\lambda_1 + \ldots + (v_n + U)\lambda_n = (v_1\lambda_1 + \ldots + v_n\lambda_n) + U = U$$

Следующий результат является непосредственным следствием только что доказанной теоремы, но ввиду его огромной важности мы тоже назовем его теоремой.

Теорема. *Если* $U \leq V$, *то*

$$\dim(V) = \dim(U) + \dim(V/U).$$

Доказательство. В самом деле, объединение любого базиса U и любого базиса V относительно U является базисом V.

Пусть T — тело, $U \leq V$ — подпространство векторного пространства над T. Тогда мощность базиса V относительно U — или, что то же самое, размерность пространства V/U — называется **коразмерностью** подпространства U в пространстве V и обозначается $\operatorname{codim}(U, V)$, или просто $\operatorname{codim}(U)$, если пространство V определено контекстом.

Следствие. *Для любого подпространства $U \leq V$ имеет место равенство*

$$\dim(V) = \dim(U) + \mathrm{codim}(U, V).$$

В частности, если $\dim(V) < \infty$*, то*

$$\mathrm{codim}(U, V) = \dim(V) - \dim(U).$$

Следствие. *Если* $U, V \leq W$ *и* $\dim(W) < \infty$*, то*

$$W = U \oplus V \qquad \Longleftrightarrow \qquad W = U + V, \quad \dim(W) = \dim(U) + \dim(V).$$

Задача. Если $U, V \leq W$ — два подпространства

i) Если $\mathrm{codim}(U, W), \mathrm{codim}(V, W) < \infty$, то $\mathrm{codim}(U \cap V, W) < \infty$.

ii) Если $U \leq V \leq W$ и $\mathrm{codim}(U, V), \mathrm{codim}(V, W) < \infty$, то $\mathrm{codim}(U, W) < \infty$. Верно ли, что

$$\mathrm{codim}(U, W) = \mathrm{codim}(U, V) + \mathrm{codim}(V, W).$$

Задача. Если $\mathrm{codim}(U, V) = n$, то существуют n линейно независимых функционалов $\phi_1, \ldots, \phi_n \in V^*$ таких, что

$$U = \mathrm{Ker}(\phi_1) \cap \ldots \cap \mathrm{Ker}(\phi_n),$$

иными словами, $\dim U^{\perp} = n$, где $U^{\perp} \leq V^*$ — ортогонал U

Задача. Пусть $U, V \leq W$ — подпространства векторного пространства над T. Тогда U и V в том и только том случае имеют общее дополнение Z, когда $\dim(U) = \dim(V)$.

Указание. Доказательство сразу сводится к случаю $\dim(W) < \infty$.

§ 9♢. Теорема о размерности ядра и образа

В настоящем параграфе мы дадим еще одну формулировку теоремы о гомоморфизме в случае, когда $R = K$ — поле. В элементарных учебниках следующий результат обычно называется **теоремой о размерности ядра и образа**, но профессиональные алгебраисты обычно сохраняют традиционное немецкое название.

Rangsatz. *Для любого линейного отображения* $\phi : U \longrightarrow V$ *имеет место равенство*

$$\dim(\mathrm{Ker}(\phi)) + \dim(\mathrm{Im}(\phi)) = \dim(U).$$

Доказательство. В самом деле, по теореме о гомоморфизме

$$\mathrm{Im}(\phi) \cong U / \mathrm{Ker}(\phi),$$

и нам остается сослаться на теорему об относительных базисах.

Опять же в наивных учебниках элементарной линейной алгебры вместо недвусмысленной ссылки на теорему о гомоморфизме в этом месте происходит невнятное бормотание, наподобие следующего. С моей точки зрения единственная цель подобных доказательств состоит в том, чтобы создать искусственные трудности студенту.

Имитация доказательства. Для удобства обозначений мы проведем доказательство в случае конечномерных пространств, хотя все рассуждения носят общий характер и сохраняют силу для произвольных пространств. Зафиксируем, прежде всего, какой-то базис $x_1, \ldots, x_m$ ядра $\mathrm{Ker}(\phi) \leq U$. Так как $x_1, \ldots, x_m$ линейно независимая система, ее можно дополнить до базиса пространства U. Пусть $x_1, \ldots, x_m, x_{m+1}, \ldots, x_n$ — получающийся таким образом базис U. Нам достаточно показать, что $\phi(x_{m+1}), \ldots, \phi(x_n)$ — базис $\mathrm{Im}(\phi)$. В самом деле, отсюда следует, что

$$\dim(\mathrm{Im}(\phi)) = n - m = \dim(U) - \dim(\mathrm{Ker}(\phi)),$$

как и утверждалось.

Докажем вначале, что $\phi(x_{m+1}), \ldots, \phi(x_n)$ порождают $\mathrm{Im}(\phi)$. В самом деле, для любого $y \in \mathrm{Im}(\phi)$ найдется такой $x \in U$, что $\phi(x) = y$. Разложим x по нашему базису пространства U:

$$x = x_1\lambda_1 + \ldots + x_m\lambda_m + x_{m+1}\lambda_{m+1} + \ldots + \lambda_n x_n.$$

Применив к этому равенству ϕ, воспользовавшись линейностью и вспомнив, что $x_1, \ldots, x_m$ лежат в ядре ϕ, получим

$$y = \phi(x) = \phi(x_{m+1})\lambda_{m+1} + \ldots + \phi(x_n)\lambda_n.$$

Докажем теперь, что $\phi(x_{m+1}), \ldots, \phi(x_n)$ линейно независимы. В самом деле, пусть

$$\phi(x_{m+1})\lambda_{m+1} + \ldots + \phi(x_n)\lambda_n = 0$$

какая-то линейная зависимость между ними. Положим

$$x = x_{m+1}\lambda_{m+1} + \ldots + x_n\lambda_n \in U.$$

По условию $\phi(x) = 0$, так что $x \in \mathrm{Ker}(\phi)$ и, следовательно, x можно разложить по $x_1, \ldots, x_m$, составляющим базис ядра, т. е. существуют такие $\lambda_1, \ldots, \lambda_m \in K$, что

$$x_1\lambda_1 + \ldots + x_m\lambda_m = x_{m+1}\lambda_{m+1} + \ldots + x_n\lambda_n.$$

Однако так как $x_1, \ldots, x_n$ линейно независимы, это означает, что

$$\lambda_1 = \ldots = \lambda_m = \lambda_{m+1} = \ldots = \lambda_n = 0.$$

что и завершает доказательство теоремы.

§ 10♢. Теорема о размерности суммы и пересечения

Сейчас мы установим один из важнейших фактов линейной алгебры над полем, являющийся обобщением принципа включения и исключения и еще одной формой теоремы Нетер об изоморфизме. Пусть U, V два подпространства векторного пространства W. Теорема Нетер утверждает, что $(U+V)/V \cong U/(U \cap V)$. В частности,

$$\dim((U+V)/V) = \dim(U/(U \cap V)).$$

Но ведь если $Y \leq X$ есть подпространство конечномерного пространства X, то

$$\dim(X/Y) = \operatorname{codim}(X, Y) = \dim(X) - \dim(Y).$$

Таким образом, если пространства U, V оба конечномерны, то и $U+V$ тоже конечномерно и, следовательно,

$$\dim(U+V) - \dim(V) = \dim(U) - \dim(U \cap V).$$

Разумеется, для бесконечных размерностей вычитание не имеет большого смысла, но после незначительного исправления формулировки этот факт продолжает оставаться верным и в общем случае. Как видно из доказательства, следующий результат является частным случаем `Rangsatz` = теоремы о размерности ядра и образа.

Теорема. *Пусть $U, V \leq W$ — два подпространства векторного пространства W. Тогда*

$$\dim(U+V) + \dim(U \cap V) = \dim(U) + \dim(V)$$

Доказательство. В первой главе мы построили точную последовательность линейных отображений

$$0 \longrightarrow U \cap V \longrightarrow U \oplus V \longrightarrow U + V \longrightarrow 0.$$

Как мы знаем из предыдущего параграфа, отсюда следует, что

$$\dim(U+V) + \dim(U \cap V) = \dim(U \oplus V),$$

как и утверждалось.

Для сравнения приведем доказательство этого факта, записанное в том стиле, как это принято в элементарных учебниках наивной линейной алгебры. Тот факт, что относительный базис V над $U \cap V$ одновременно является относительным базисом $U+V$ над U озвучивается примерно так.

Имитация доказательства. Для удобства обозначений мы проведем доказательство в случае конечномерных пространств, хотя все рассуждения носят общий характер и сохраняют силу для произвольных пространств. Пусть $w_1, \dots, w_l$ — какой-то базис пространства W. Так как векторы $w_1, \dots, w_l$ линейно независимы, то их можно дополнить до базиса пространств U и V. Пусть $u_1, \dots, u_m$ и $v_1, \dots, v_n$ — дополнения $w_1, \dots, w_l$ до базисов пространств U и V, соответственно. Мы утверждаем, что

$$X = (w_1, \dots, w_l, u_1, \dots, u_m, v_1, \dots, v_n)$$

представляет собой базис пространства $U+V$. В этом случае $(l+m+n)+l = (l+m)+(l+n)$, как и утверждалось.

В самом деле, так как $U, V \leq \langle X \rangle$, то $U+V \leq \langle X \rangle$, так что X действительно порождает $U+V$ и нам остается только доказать линейную независимость. Рассмотрим линейную зависимость

$$w_1\alpha_1 + \dots + w_l\alpha_l + u_1\beta_1 + \dots + u_m b_m + v_1\gamma_1 + \dots + v_n\gamma_n = 0,$$

где $\alpha_1, \dots, \alpha_l, \beta_1, \dots, \beta_m, \gamma_1, \dots, \gamma_n \in K$. Мы хотим показать, что эта линейная зависимость тривиальна. Перенося все слагаемые $\gamma_i v_i$ в правую часть мы получаем равенство

$$z = w_1\alpha_1 + \dots + w_l\alpha_l + u_1\beta_1 + \dots + u_m\beta_m = -v_1\gamma_1 - \dots - v_n\gamma_n,$$

где все слагаемые в левой части принадлежат U, а все слагаемые в правой части принадлежат V. Тем самым $z \in U \cap V$ и, значит, может быть разложен по базису $w_1, \dots, w_l$ этого пространства. В силу линейной независимости $w_1, \dots, w_l, u_1, \dots, u_m$ получаем $z = w_1\alpha_1 + \dots + w_l\alpha_l$ или, что то же самое $\beta_1 = \dots = \beta_m = 0$. Таким образом, наша линейная зависимость свелась к

$$w_1\alpha_1 + \dots + w_l\alpha_l + v_1\gamma_1 + \dots + v_n\gamma_n = 0,$$

но ведь векторы $w_1, \dots, w_l, v_1, \dots, v_n$ тоже линейно независимы, так что $\alpha_1 = \dots = \alpha_l = \gamma_1 = \dots = \gamma_n = 0$, как и утверждалось.

Следствие. *Если $U, V \leq W$, то*

$$\dim(U \cap V) \geq \dim(U) + \dim(V) - \dim(W).$$

Задача. Докажите, что если U, V два подпространства конечной коразмерности в W, то $U \cap V$ тоже имеет конечную коразмерность и

$$\operatorname{codim}(W, U+V) + \operatorname{codim}(W, U \cap V) = \operatorname{codim}(W, U) + \operatorname{codim}(W, V).$$

Как Вы думаете, продолжает ли это равенство оставаться справедливым для подпространств бесконечной коразмерности?

§ 11♡. Векторные пространства над $\mathbb{F}_p$

Сейчас мы убедимся в том, что векторное пространство над $\mathbb{F}_p$ это то же самое, что **элементарная абелева p-группа**, т.е. абелева группа, каждый элемент которой $x \neq e$ имеет порядок p.

Теорема. *Категория векторных пространств над $\mathbb{F}_p$ совпадает с категорией элементарных абелевых p-групп.*

В переводе на общечеловеческий язык, эта теорема утверждает *в точности* две следующие вещи.

1) Подлежащая группа $\mathbb{F}_p$-векторного пространства является элементарной абелевой p-группой и, обратно, на любой элементарной абелевой p-группе A существует единственная структура $\mathbb{F}_p$-векторного пространства.

2) Для любых двух элементарных абелевых p-групп

$$\operatorname{Hom}(A, B) = \operatorname{Hom}_{\mathbb{F}_p}(A, B).$$

Доказательство. 1) Если A — векторное пространство над $\mathbb{F}_p$, то для любого $x \in A$ имеем $px = 0$. Обратно, если A — элементарная абелева p-группа, то $p\mathbb{Z}$ лежит в ядре канонического гомоморфизма $\mathbb{Z} \longrightarrow \operatorname{End}_{\mathbb{Z}}(A)$. Таким образом, мы получаем гомоморфизм $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \longrightarrow \operatorname{End}_{\mathbb{Z}}(A)$. Так как для любого простого p может существовать не более одного такого гомоморфизма, это полностью определяет структуру $\mathbb{F}_p$-векторного пространства на A.

2) По определению правая часть содержится в левой. Для доказательства обратного включения нужно вспомнить, что $\operatorname{Hom}(A, B) = \operatorname{Hom}_{\mathbb{Z}}(A, B)$.

Эта теорема показывает, что к элементарным абелевым p-группам можно применять все результаты линейной алгебры над полем!

§ 12♡. Векторные пространства над $\mathbb{Q}$

Абелева группа A называется

• **группой без кручения**, если все гомотетии $\theta_n \colon A \longrightarrow A$, $x \mapsto nx$, где $n \in \mathbb{Z}$, *инъективны*,

• **делимой**, если они *сюръективны*,

• **однозначно делимой**, если они *биективны*.

Иными словами, в группе без кручения можно сокращать на ненулевые целые числа: если $nx = ny$, то $n(x - y) = 0$ и, если $n \neq 0$, то $x - y = 0$ или, что то же самое, $x = y$. В делимой группе для любого $x \in A$ и любого $n \in \mathbb{Z}^\bullet$ существует $y \in A$ такое, что $ny = x$. По определению однозначно делимая группа — это делимая группа без кручения. В однозначно делимой группе для каждых таких x, n существует ровно один y такой, что $ny = x$. Еще раз убедимся в этом: если $ny = nz = x$ для двух элементов $y, z \in A$, то, так как A без кручения, то $y = z$.

Теорема. *Категория векторных пространств над* $\mathbb{Q}$ *совпадает с категорией однозначно делимых абелевых групп.*

Как мы уже знаем из предыдущего параграфа, эта теорема утверждает *в точности* две следующие вещи.

1) Подлежащая группа $\mathbb{Q}$-векторного пространства является однозначно делимой абелевой группой и, обратно, на любой однозначно делимой абелевой группе A существует единственная структура $\mathbb{Q}$-векторного пространства.

2) Для любых двух однозначно делимых абелевых групп

$$\mathrm{Hom}(A,B)=\mathrm{Hom}_{\mathbb{Q}}(A,B).$$

Доказательство. 1) Если A — векторное пространство над $\mathbb{Q}$, то гомотетия $x\mapsto nx$, $n\in\mathbb{Z}^\bullet$, биективна на A. Обратно, пусть A — однозначно делимая абелева группа. Так как для $A=0$ утверждение очевидно, в дальнейшем мы сичтаем, что $A\neq 0$. По условию умножения на n, $n\in\mathbb{Z}\bullet$, являются обратимыми элементами кольца $\mathrm{End}_{\mathbb{Z}}(A)$. Ясно, что гомоморфизм $\mathbb{Z}\longrightarrow\mathrm{End}_{\mathbb{Z}}(A)$, сопоставляющий $n\in\mathbb{Z}$ соответствующую гомотетию θ_n, инъективен. (В самом деле, если $mx=nx$ для всех $x\in A$, то $(m-n)x=0$; для $A\neq 0$ предположение $m\neq n$ противоречило бы отсутствию кручения в A.) Таким образом, $\mathbb{Z}^\bullet\subseteq\mathrm{Aut}_{\mathbb{Z}}(A)$ и, значит, гомоморфизм $\mathbb{Z}\longrightarrow\mathrm{End}_{\mathbb{Z}}(A)$ продолжается до гомоморфизма $\mathbb{Q}\longrightarrow\mathrm{End}_{\mathbb{Z}}(A)$, $m/n\mapsto\theta_m\theta_n^{-1}$. Так как существует не более одного такого гомоморфизма, это полностью определяет структуру $\mathbb{Q}$-векторного пространства на A.

2) По определению правая часть содержится в левой. Обратно, пусть $\phi: A\longrightarrow B$ гомоморфизм групп, т.е. $\mathbb{Z}$-линейное отображение. Мы хотим показать, что ϕ будет $\mathbb{Q}$-линейным. Пусть $x\in A$, $m/n\in\mathbb{Q}$. Так как $nf(m/n\cdot x)=f(mx)=mf(x)=(n\cdot m/n)f(x)=n(m/n\cdot f(x))$ и группа B однозначно делима, то $f(m/n\cdot x)=m/n\cdot f(x)$.

Эта теорема показывает, что к однозначно делимым абелевым группам можно применять все результаты линейной алгебры над полем! Так как все векторные пространства данной бесконечной размерности изоморфны, то теория однозначно делимых абелевых групп категорична в несчетных мощностях. Например, все однозначно делимые абелевы группы мощности континуум изоморфны. Этот общий принцип можно проиллюстрировать например, так.

Следствие. *Все аддитивные группы* $\mathbb{R}^n$ *и* $\mathbb{C}^n$ *при* $n\geq 1$ *изоморфны между собой.*

Любая делимая абелева группа есть прямая сумма группы кручения и бесконечно делимой группы. Например, мультипликативная группа комплексных чисел $\mathbb{C}^*$ и группа углов

$$\mathbb{T}=\{z\in\mathbb{C}^*\mid |z|=1\},$$

состоящая из комплексных чисел модуля 1, имеют одну и ту же счетную группу кручения, состоящую из всех корней из 1. Тем самым, фактор-группа по подгруппе кручения и в том и в другом случае имеет мощность континуум. Это значит, что мы получаем такую еще более спектакулярную иллюстрацию нашей основной теоремы.

Следствие. *Имеет место изоморфизм мультипликативных групп*

$$\mathbb{C}^* \cong \mathbb{T}.$$

Я уверен, что не только студенты, но и большинство математиков-неспециалистов не подозревают о существовании этого изоморфизма. Разумеется, такой изоморфизм не может быть непрерывным относительно обычной вещественной/комплексной топологии.

§ 13♡. Многочлены Гаусса

Сколько имеется базисов в n-мерном пространстве над полем из q элементов, сколько там m-мерных подпространств и т.д.? В следующем параграфе мы ответим на все подобные вопросы. Для этого мы сейчас введем очень широкое обобщение биномиальных коэффициентов — многочлены Гаусса.

Определение. Многочленом Гаусса *называется*

$$\binom{n}{m}_x = \frac{(x^n-1)\dots(x^{n-m+1}-1)}{(x^m-1)\dots(x-1)}$$

.

Так как все многочлены в числителе и знаменателе нормированные, то $\binom{n}{m}_q$ — нормированный многочлен с целыми коэффициентами степени $m(n-m)$ по q. Из определения очевидно, что

$$\binom{n}{n}_x = 1, \qquad \binom{n}{m}_x = \binom{n}{n-m}_x.$$

Обычно дополнительно полагают

$$\binom{n}{m}_x = 0, \qquad n \in \mathbb{N}_0, \quad m < 0 \ \text{ или } \ m > n.$$

Задача. Проверьте, что гауссовы коэффициенты удовлетворяют следующим **треугольным рекуррентным соотношениям**:

$$\binom{n}{m}_x = \binom{n-1}{m-1}_x + x^m\binom{n-1}{m}_x = x^{n-m}\binom{n-1}{m-1}_x + \binom{n-1}{m}_x.$$

В случае $x=1$ эти соотношения подозрительно напоминают треугольное рекуррентное соотношение между биномиальными коэффициентами.

Задача. Убедитесь, что

$$\binom{n}{m}_1 = \binom{n}{m}$$

Решение. Проще всего посчитать значение $\binom{n}{m}_x$ в 1 по **правилу л'Опиталя**. Взяв m раз производные числителя и знаменателя в определении гауссова многочлена, и подставив в них 1, мы как раз и получим биномиальный коэффициент.

Часто удобно восстановить симметрию между m и $n-m$ в определении гауссова коэффициента. А именно, введем следующий многочлен от x

$$\Psi_n(x) = (x^n - 1)(x^{n-1} - 1)\dots(x-1),$$

являющийся q-аналогом факториала. Тогда очевидно, что

$$\binom{n}{m}_x = \frac{\Psi_n(x)}{\Psi_m(x)\Psi_{n-m}(x)}.$$

Следующая теорема описывает разложение гауссовых многочленов на неприводимые. Оказывается, их неприводимыми множителями являются *попарно различные* круговые многочлены Φ_l.

Теорема. *Разложение многочленов Гаусса на неприводимые в* $\mathbb{Z}[x]$ *имеет вид*

$$\binom{n}{m}_x = \prod_{l=1}^{n} \Phi_l^{e(l)},$$

где

$$e(l) = \left\lfloor \frac{n}{d} \right\rfloor - \left\lfloor \frac{m}{d} \right\rfloor - \left\lfloor \frac{n-m}{d} \right\rfloor$$

Замечание. Ясно, что всегда $e(l) = 0$ или 1. При этом $e(l) = 1$ в том и только том случае, когда сумма наименьших неотрицательных остатков при делении m и $n-m$ на l будет $\geq l$. В частности, так как остаток при делении любого целого на 1 равен 0, то $\Phi_1 = x - 1$ в разложение $\binom{n}{m}_x$ не входит, так что эффективно произведение в теореме начинается с $l = 2$. Многочлен же $\Phi_2 = x + 1$ входит в разложение $\binom{n}{m}_x$ когда n четное, а m нечетное.

Следствие. *При всех* $0 \leq m \leq n$ *многочлен Гаусса* $\binom{n}{m}_x$ *является возвратным.*

Доказательство. Все круговые многочлены, кроме Φ_1, являются возвратными, а Φ_1 в $\binom{n}{m}_x$ не входит. Осталось заметить — вспомнить? — что произведение возвратных многочленов тоже возвратный многочлен.

§ 14♡. Линейная алгебра над конечным полем

А теперь то, ради чего, собственно, и вводились гауссовы многочлены. Пусть $V = \mathbb{F}_q{}^n$ — n-мерное векторное пространство над полем $\mathbb{F}_q$ из q элементов. Сейчас мы найдем количество базисов V, количество m-мерных подпространств в V и тому подобные вещи. Они выражаются в терминах значений $\binom{n}{m}_q$ гауссовых многочленов в q.

Теорема. *Количество систем m штук линейно независимых векторов в n-мерном пространстве над полем из q элементов равно*

$$(q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{m-1}) = q^{m(m-1)/2}\frac{\Psi_n(q)}{\Psi_{n-m}(q)}.$$

Доказательство. Всего в n-мерном пространстве над полем из q элементов имеется q^n штук векторов. Проведем следующее итеративное рассуждение.

• В качестве первого вектора линейно независимой системы может фигурировать любой *ненулевой* вектор, значит для первого вектора имеется q^n-1 возможность.

• В качестве второго вектора линейно независимой системы может фигурировать любой вектор *линейно независимый* от первого. Кратные одного ненулевого вектора образуют *прямую*, на которой q точек, значит для второго вектора имеется q^n-q возможностей.

• В качестве третьего вектора линейно независимой системы может фигурировать любой вектор *линейно независимый* от первого и второго. Линейные комбинации двух линейно независимых векторов образуют *плоскость*, на которой q^2 точек, значит для третьего вектора имеется q^n-q^2 возможностей.

Продолжая действовать таким образом мы дойдем до следующей ситуации.

• В качестве m-го вектора линейно независимой системы может фигурировать любой вектор *линейно независимый* от предыдущих $m-1$ векторов. Линейные комбинации $m-1$ линейно независимого вектора образуют $(m-1)$-мерное пространство, на котором q^{m-1} точек, значит для последнего вектора имеется q^n-q^{m-1} возможностей.

Остается применить правило произведения

Следствие 1. *Количество базисов в n-мерном пространстве над полем из q элементов равно*

$$(q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{n-1}) = q^{n(n-1)/2}\Psi_n(q).$$

Обратите внимание, что базисов в n-мерном пространстве столько же, сколько обратимых матриц степени n. Таким образом, только что приведеннная формула есть в действительности формула для порядка полной линейной группы $\mathrm{GL}(n,\mathbb{F}_q)$.

Следствие 2. *Количество m-мерных подпространств в n-мерном пространстве над полем из q элементов равно* $\binom{n}{m}_q$

Доказательство. Каждая линейно независимая система из m штук векторов порождает m-мерное подпротсранство и является в нем базисом. Таким образом, в теореме мы вычислили *общее* количество базисов всех m-мерных подпространств в n-мерном пространстве. Остается лишь разделить его на количество базисов *данного* m-мерного пространства.

Отступление. Это следствие подчеркивает аналогию между множествами и векторными пространствами. Сравнение с известной формулой для колдичества m-элементных подмножеств n-элементного множества показывает, что на множества следует смотреть просто как на векторные пространства над полем из 1 элемента. При этом размерность такого пространства равна его мощности, а базис состоит из всех элементов. Такая точка зрения чрезвычайно плодотворна для комбинаторики, так как рассмотрение векторных пространств над произвольным конечным полем $\mathbb{F}_q$ с последующей специализацией $q = 1$ обычно значительно проще, чем рассмотрение случая $q = 1$ самого по себе: многочлены проще, чем целые числа, потому что в них больше структуры.

Задача. Сколько m-мерных подпространств n-мерного векторного пространства над полем из q элементов имеют нулевое пересечение с фиксированным l-мерным подпространством?

Задача. Разложим n-мерное пространство V над полем из q элементов в прямую сумму l-мерного подспространства U и $(n - l)$-мерного подпространства W. Сколько m-мерных подпространств в V имеют нулевое пересечение как с U, так и с W?

Глава 4. ЛИНЕЙНАЯ АЛГЕБРА В СОДЕРЖАТЕЛЬНЫХ ПРИМЕРАХ

В деревне бог живет не по углам,
Как думают насмешники, а всюду.

Иосиф Бродский, *Остановка в пустыне*

Смысл математического понятия далеко не содержится в его формальном определении. Не меньше — скорее больше — дает набор основных примеров, являющихся для математика одновременно и **мотивировкой**, и **содержательным определением**, и **смыслом** понятия.

Игорь Шафаревич, [Sha]

Pozycja analizy w matematice jest szczególna: zupełnie inna niż algebry, teorii liczb, teorii mnogości ... Nie jest dyscypliną samodzielną: oparta jest na topologii i algebrze. — Анализ занимает в математике совершенно особое положение. В отличие от алгебры, теории чисел или теории множеств, он не является самостоятельной дисциплиной, а целиком базируется на топологии и алгебре.

Krzysztof Maurin, *Analiza,* I. *Elementy*

В настоящей главе мы приведем несколько классических примеров модулей и векторных пространств, возникающих в элементарной математике, главным образом, в анализе. Разумеется, в классическом анализе линейная алгебра живет не по углам, поэтому в настоящей главе мы не стремимся к систематичности, а ограничиваемся несколькими очевидными примерами, которые должны настроить сознание студента на поиск изученных нами понятий и явлений в самых простых и классических ситуациях.

§ 1♡. Пространства последовательностей

Все рассмотренные в книге III кольца последовательностей содержат константы и, таким образом, в частности, как сами эти кольца, так и идеалы в них являются векторными пространствами над K. В частности, в книге III нам уже встречались:

• $S(\mathbb{R})$ — пространство всех последовательностей;

• $S_b(\mathbb{R})$ — пространство всех *ограниченных* последовательностей;

• $S_c(\mathbb{R})$ — пространство всех *сходящихся* последовательностей;

• $S_v(\mathbb{R})$ — пространство всех *исчезающих* последовательностей (иными словами, последовательностей, сходящихся к 0);

• $S_o(\mathbb{R})$ — пространство всех *финитных* последовательностей (все члены которых начиная с некоторого места равны 0);

• $S_s(\mathbb{R})$ — пространство всех *стабильных* последовательностей (в которых все члены, кроме конечного их числа, равны одному и тому же $c \in \mathbb{R}$).

Упражнение. Перечислите все включения между этими пространствами.

Наряду с этими подпространствами, которые в действительности являются подкольцами, в анализе рассматриваются и такие классы последовательностей, которые не являются кольцами относительно операции умножения функций, но, тем не менее, образуют векторные пространства.

Рассмотрим множество l^p, состоящее из всех последовательностей $x = (x_i)$, $i \in \mathbb{N}$, для которых ряд $\sum\limits_{i\in\mathbb{N}} |x_i|^p$ сходится.

$$N_p(x) = \Big(\sum_{i\in\mathbb{N}} |x_i|^p\Big)^{1/p}.$$

Одно из важнейших неравенств анализа, **неравенство Минковского**, утверждает, что

$$N_p(x+y) \leq N_p(x) + N_p(y).$$

Таким образом, если $N_p(x), N_p(y) < \infty$, то $N_p(x+y) < \infty$. так что из неравенства Минковского вытекает, что l^p является векторным пространством. Вот три классических примера пространств l^p.

• Пространство l^1 состоит из *абсолютно* сходящихся последовательностей.

• Пространство l^2 состоит из последовательностей $x = (x_i)$, для которых $\sum\limits_{i\in\mathbb{N}} |x_i|^2 < \infty$

• Пространство l^∞ совпадает с пространством $S_b(\mathbb{R})$ ограниченных последовательностей.

§ 2♡. Пространства функций: общие места

Начнем с самой общей ситуации, которую мы уже упоминали в главе 1. Пусть X — произвольное множество, а R — коммутативное кольцо. Рассмотрим множество функций $R^X = \mathrm{Map}(X, R)$. Как мы уже знаем, относительно обычного сложения функций и операции умножения функции на константу:

$$(f+g)(x) = f(x) + g(x), \qquad (\lambda f)(x) = \lambda f(x).$$

В дальнейшем, говоря о **пространствах функций**, мы имеем в виду подпространства в V. В следующем параграфе мы приведем несколько наиболее известных примеров таких подпространств.

• **Прямые суммы**. Разложению $X = X_1 \sqcup \ldots \sqcup X_n$ множества X в дизъюнктное объединение отвечает разложение пространства функций на нем в прямую сумму

$$R^{X_1 \sqcup \ldots \sqcup X_n} \cong R^{X_1} \oplus \ldots \oplus R^{X_n}.$$

Изоморфизм между этими пространствами устанавливается посредством

$$f \mapsto (f|_{X_1}, \ldots, f|_{X_n}).$$

В частности, если множество $X = \{x_1, \ldots, x_n\}$ конечно, описанная конструкция устанавливает изоморфизм $R^X \longrightarrow R^n = R \oplus \ldots \oplus R$, $f \mapsto (f(x_1), \ldots, f(x_n))$.

• **Фактор-пространства**. Каждому подмножеству $Y \subseteq X$ соответствует подпространство $I(Y) \leq R^X$, состоящее из функций обращающихся в 0 на Y:

$$I(Y) = \{f \in R^X \mid \forall y \in Y,\ f(y) = 0\}.$$

В этом случае фактор-пространство $R^X/I(Y)$ естественно отождествляется с пространством R^Y. Мы не развиваем здесь эту тему, но многие пространства классического анализа как фактор-пространства пространства R^V.

• **Тензорные произведения**. В части 5 мы рассматриваем еще одну важнейшую конструкцию над векторными пространствами, тензорные произведения. В случае, когда хотя бы одно из множеств X или Y *конечно*, имеет место изоморфизм $R^{X \times Y} = R^X \otimes R^Y$.

§ 3♡. Пространства функций: примеры

В настоящей главе мы опишем некоторые простейшие примеры встречающихся в анализе пространств функций.

1. Простейшие примеры. Все рассмотренные нами в книге III кольца вещественных функций содержат константы и, таким образом, в частности, как сами эти кольца, так и идеалы в них являются векторными пространствами над $\mathbb{R}$. Мы не будем повторять здесь все эти примеры, а ограничимся лишь примерами, связанными с кольцом непрерывных функций. Чаще всего возникает случай, когда X — локально компактное хаусдорфово топологическое пространство, дииференцируемое многообразие или что-нибудь в таком духе. Начинающий должен представлять себе, что речь здесь идет об $X = \mathbb{R}, \mathbb{R}^n, [0,1]$ или $\mathbb{Z}$. Тогда следующие множества являются векторными пространствами над $\mathbb{R}$.

• Множество $A(I)$ функций, имеющих предел в каждой точке I.

• Множество $B(I)$ ограниченных функций на I.

• Множество $C(I)$ непрерывных функций на I.

• Множество $BC(I) = B(I) \cap C(I)$ непрерывных ограниченных функций.

• Множество

$$C_c(X) = \{f \in C(X) \mid \mathrm{Supp}(f) \text{ компактен}\}.$$

непрерывных функций с компактным носителем.

• Множество $C_0(X)$ непрерывных функций, обращающихся в 0 на бесконечности.

• Множество $\mathrm{C}^m(I)$ m раз непрерывно дифференцируемых функций на I.

• Множество $\mathrm{C}^\infty(I)$ бесконечно дифференцируемых функций на I.

• Множество $\mathrm{C}^\omega(I)$ аналитических функций на I.

• Множество $V(0,1)$ функций ограниченной вариации на $I=[0,1]$, см., например[11].

В действительности все эти классы функций замкнуты относительно обычного умножения функций и, тем самым, образуют $\mathbb{R}$-алгебры. С другой стороны, многие рассматриваемых в анализе классы функций не являются кольцами относительно операции умножения функций, но, тем не менее, образуют векторные пространства.

2. Классы функций, не являющихся векторными пространствами. Многие основные рассматриваемые в анализе классы функций являются векторными пространствами. Однако довольно часто встречаются и такие классы функций, которые векторных пространств не образуют, так как сумма двух функций из этих классов — или произведение таких функций на *отрицательное* вещественное число — не попадают в этот класс. Таковы, например, классы

• монотонных функций на интервале $[a,b]$;

• выпуклых функций на интервале $[a,b]$;

• полунепрерывных[12] функций на интервале $[a,b]$;

• *всех* периодических функций на $\mathbb{R}$ — функции *фиксированного* периода образуют пространство и даже $\mathbb{R}$-алгебру! Мы вернемся к обсуждению этого примера в § ?.

• функций на интервале $[a,b]$, квадрат которых интегрируем по Риману[13] (или по Лебегу[14]);

3. Пространство решений линейного однородного дифференциального уравнения. Рассмотрим линейных дифференциальный оператор $D\in\mathbb{R}\left[\dfrac{d}{dx}\right]$ с постоянными коэффициентами. Тогда множество функций f, являющихся решениями однородного дифференциального уравнения $Df=0$ всегда образует векторное пространство, но очень редко является кольцом. В действительности, это верно для уравнений с произвольными гладкими (но не обязательно постоянными) коэффициентами:

$$\frac{d^nf}{d^nx}+g_{n-1}(t)\frac{d^{n-1}f}{d^{n-1}x}+\ldots+g_1\frac{df}{dx}+g_0=0,$$

где $g_0,\ldots,g_{n-1}$ суть фиксированные гладкие функции.

[11] У.Рудин, Основы математического анализа. 2-е изд., М., Мир, 1976, 319с. теорема 6.24.

[12] Б.Гелбаум, Дж. Олмстед, Контр-примеры в анализе. — М., Мир, 1967, с. 1—251; стр.220—221.

[13] Б.Гелбаум, Дж.Олмстед, ibid., стр.222.

[14] Б.Гелбаум, Дж.Олмстед, ibid., стр.222–223.

§ 4♡. Модули над кольцами функций

В этом параграфе мы объясним почему даже с точки зрения приложений в дисциплинах аналитического цикла при изучении линейной алгебры совершенно неестественно ограничиваться рассмотрением векторных пространств. Дело в том, что *центральную* роль в анализе, геометрии и всех опирающихся на них областях математики играют геометрические объекты на (дифференцируемом, гладком, аналитическом, комплексном или алгебраическом) многообразии X. В отличие от локальных понятий, таких как касательный или кокасательный вектор, геометрические объекты, такие как векторные и тензорные поля, дифференциальные формы, и т.д. меняются от точки к точке. Множество всех касательных векторов в точке — касательное пространство — является векторным пространством, в классическом случае пространством над $\mathbb{R}$ или над $\mathbb{C}$. Множество всех векторных полей — касательное расслоение — и вообще множество всех геометрических объектов любого фиксированного типа тоже является векторным пространством над $\mathbb{R}$ или над $\mathbb{C}$. Тем не менее, во всех этих случаях гораздо естественнее рассматривать эти множества не как векторные пространства, а как модули над соответствующим кольцом функций.

Вот самая общая (и поэтому самая простая) версия этой конструкции. Пусть X — произвольное множество, K — поле, а V — векторное пространство над K. Как мы знаем, тогда множество $R = K^X$ всех K-значных функций на X образует кольцо относительно обычных сложения и умножения функций. Рассмотрим теперь множество $M = V^X$ всех отображений $X \longrightarrow V$ (как сказали бы аналисты, 'векторно-значных функций на V'). Определим операции на M следующим образом. Для любых $\phi, \psi \in M$, $f \in R$ положим

$$(\phi + \psi)(x) = \phi(x) + \psi(x), \qquad (f\phi)(x) = f(x)\phi(x).$$

Легко видеть, что эти операции превращают M в R-модуль.

Отступление. В алгебраической геометрии после Гротендика рассматривается еще гораздо более общая конструкция, в которой само поле K тоже зависит от точки $x \in X$. Иными словами, для каждой точки $x \in X$ рассматривается поле K_x. Обозначим через R множество функций $f : X \longrightarrow \bigcup K_x$ таких, что $f(x) \in K_x$ для каждого $x \in X$. Относительно обычных операций над функциями R образует кольцо изоморфное прямому произведению полей K_x, $x \in X$. Зафиксируем теперь для каждого $x \in X$ векторное пространство V_x над K_x и рассмотрим множество M функций $f : X \longrightarrow \bigcup V_x$ таких, что $f(x) \in V_x$ для каждого $x \in X$. Теперь уже M не является векторным пространством (над чем?) Тем не менее, M, конечно, по-прежнему продолжает быть R-модулем.

Вот несколько примеров применения этой конструкции.

• Векторные поля на многообразии образуют модуль над кольцом функций.

• Дифференциальные формы заданной размерности на многообразии образуют модуль над кольцом функций.

• Вообще, тензорные поля *любого* данного типа, удовлетворяющие любому условию симметрии, образуют модуль над кольцом функций на многообразии.

А вот пример несколько другого рода.

• Меры на многоообразии X являются модулем над кольцом функций на нем.

§ 5♡. Модули над кольцом многочленов

Пусть $R = K[x]$ — кольцо многочленов от одной переменной над полем K. Что такое модуль над кольцом R? Сужая скаляры вдоль вложения $K \hookrightarrow K[x]$ мы видим, что каждый такой модуль является векторным пространством над K. С другой стороны, так как действие x на V коммутирует с константами, то гомотетия $\phi = \theta_x : V \longrightarrow V$, $u \mapsto xu$, представляет собой K-линейный оператор $\phi \in \mathrm{End}_K(V)$. Таким образом, умножение на x можно рассматривать как линейный оператор на векторном пространстве V. Обратно, в силу универсального свойства кольца многочленов для любого такого линейного оператора $\phi \in \mathrm{End}_K(V)$ существует единственный гомоморфизм K-алгебр $K[x] \longrightarrow \mathrm{End}_K(V)$, отображающий x в ϕ. В этом случае x^m перейдет в ϕ^m — напомним, что умножением в $\mathrm{End}_K(V)$ является композиция и $\phi^0 = \mathrm{id}_V$. Кроме того, так как это гомоморфизм K-алгебр, то любая линейная комбинация степеней x^m с коэффициентами из K перейдет в линейную комбинацию ϕ^m с теми же коэффициентами.

Резюмируя только что сказанное, мы можем констатировать, что

• $K[x]$-модуль это в точности векторное пространство V над K вместе с заданным на нем K-эндоморфизмом ϕ.

В дальнейшем мы будем обычно задавать $K[x]$-модуль как пару (V, ϕ).

Тем самым, изучение линейных операторов в векторных пространствах над полями эквивалентно изучению $K[x]$-модулей. В части 3 для *конечномерных* пространств мы будем широко пользоваться этим соответствием как в ту, так и в другую сторону. Спектральная теория операторов в бесконечномерных пространствах в общем случае штука довольно сложная.

Обобщается ли это соответствие на случай нескольких операторов? Да, если помнить, что в кольце $K[x, y]$ многочленов от коммутирующих переменных x, y выполняется равенство $xy = yx$, а для операторов это равенство нужно отдельно постулировать.

• Модуль над $K[x, y]$ это векторное пространство V над K вместе с парой коммутирующих операторов ϕ, ψ.

• Модуль над $K\langle x, y\rangle$ это векторное пространство V над K вместе с парой операторов ϕ, ψ.

§ 6♡. Модули над кольцом дифференциальных операторов

Рассмотрим кольцо линейных дифференциальных операторов с постоянными коэффициентами $K\Big[\dfrac{d}{dx_1}, \dots, \dfrac{d}{dx_n}\Big]$. Оно действует в пространстве функций — полиномиальных, экспоненциальных многочленов, бесконечно дифференцируемых, финитных, ... Резюмируем некоторые важнейшие примеры модулей над кольцом $K\left[\dfrac{d}{dx}\right]$, разумеется, все они обощаются на случай произвольного числа переменных. Во всех этих примерах $\dfrac{d}{dx}$ действует как дифференцирование, $\dfrac{d}{dx}f = f'$, где f' есть производная f. Как известно, в случае многочленов, рациональных функций и формальных степенных рядов производная определена над произвольным полем K. Для остальных случаев можно считать, что $K = \mathbb{R}$ или $\mathbb{C}$. Вот некоторые важнейшие примеры $K\left[\dfrac{d}{dx}\right]$-модулей.

- Кольцо многочленов $K[x]$.
- Поле рациональных дробей $K[x]$.
- Кольцо формальных степенных рядов $K[[x]]$.
- Поле формальных рядов Лорана $K((x))$.
- Кольцо $\mathrm{Expo}_{\mathbb{R}}$ экспоненциальных многочленов.
- Кольцо $C^{\infty}(\mathbb{R})$ бесконечно дифференцируемых функций.

Можно было бы привести многие десятки дальнейших примеров такого рода.

К обобщению первого из приведенных выше примеров на случай нескольких переменных мы будем постоянно обращаться в иллюстративных целях в дальнейшем.

- Кольцо $A = K[x_1, \ldots, x_n]$ многочленов от n переменных, рассматриваемое как модуль над кольцом линейных дифференциальных операторов с постоянными коэффициентами $R = K\left[\dfrac{\partial}{\partial x_1}, \ldots, \dfrac{\partial}{\partial x_n}\right]$. А именно, мы полагаем $D \cdot f = Df$

Хотя кольцо A и R изоморфны, структура A как модуля над собой и структура A как модуля над R абсолютно различны. Например, ${}_AA$ — модуль без кручения, в то время как ${}_RA$ — модуль кручения. Модуль ${}_AA$ — циклический модуль, порожденный элементом 1, в то время как ${}_RA$ не является даже конечно порожденным.

Подлинное чудо операционного исчисления состоит в том, что преобразование Фурье или преобразование Лапласа устанавливают изоморфизм между модулями, на одном из которых $K[x_1, \ldots, x_n]$ действует посредством умножения, а на втором — посредством дифференцирования.

§ 7♠. Пространство, порожденное сдвигами и растяжениями функции

В этом параграфе мы дадим совсем простую характеризацию многочленов и экспоненциальных многочленов в терминах линейной алгебры.

1. Сдвиги и растяжения. Напомним, что группа $\mathbb{R}^+$ действует на пространствах функций $\mathbb{R} \longrightarrow \mathbb{R}$ и $\mathbb{C}^{\mathbb{R}}$ посредством сдвигов. А именно, для $a \in \mathbb{R}$ и $f \in \mathbb{C}^{\mathbb{R}}$ обозначим через $T_a f$ функцию, определенную равенством $T_a f(x) = f(x-a)$. Про эту функцию говорят, что она получается из f **сдвигом на** a (sic!) При этом $T_{a+b} = T_a T_b$ и $T_0 = \mathrm{id}$, так что это и в самом деле групповое действие.

Аналогично, группа $\mathbb{R}^*$ действует на пространстве функций $\mathbb{R} \longrightarrow \mathbb{C}$ посредством растяжений. А именно, для $a \in \mathbb{R}^*$ и $f \in \mathbb{C}^{\mathbb{R}}$ обозначим через $H_a f$ функцию, определенную равенством $H_a f(x) = f(a^{-1}x)$. Про эту функцию говорят, что она получается из f **растяжением в** a **раз** (sic!) При этом $H_{ab} = H_a H_b$ и $H_1 = \mathrm{id}$, так что это тоже групповое действие.

Предостережение. Сдвиги и растяжения функций получаются из трансляций и гомотетий аргументов (отсюда обозначения T и H). Но действие на функциях **контравариантно** по отношению действию на аргументах! Когда мы сдвигаем аргумент функции на a **вправо**, график функции сдвигается на a **влево**. Когда мы **растягиваем** аргумент функции в a раз, график функции **сжимается** в a раз. Поэтому путать трансляции и сдвиги совершенно недопустимо!

2. Характеризация экспоненциальных многочленов. Пусть $f \in \mathbb{R}^{\mathbb{R}}$. Обозначим через $\mathrm{Shift}(f)$ подпространство, порожденное всеми сдвигами функции f:

$$\mathrm{Shift}(f) = \langle T_a f, a \in \mathbb{R} \rangle.$$

Естественно возникает вопрос, когда это пространство конечномерно? Легко привести два примера функций, для которых $\mathrm{Shift}(f)$ конечномерно.

Задача. Докажите, что если f — полиномиальная функция степени n, то $\mathrm{Shift}(f)$ совпадает с пространством всех полиномиальных функций степени $\leq n$.

Задача. Докажите, что для любого $\lambda \in \mathbb{C}$ экспоненциальная функция $f : e \mapsto e^{\lambda x x}$ является **собственной функцией** всех сдвигов, т.е. $T_a f = \mu f$ для подходящего $\mu \in \mathbb{C}$. Иными словами, пространство $\mathrm{Shift}(f)$ одномерно.

Задача. Докажите, что функции, для которых $\mathrm{Shift}(f)$ конечномерно, образуют $\mathbb{C}$-алгебру.

Иными словами, утверждается, что если пространства $\mathrm{Shift}(f)$ и $\mathrm{Shift}(g)$ конечномерны, то пространства $\mathrm{Shift}(f+g)$, $\mathrm{Shift}(fg)$ и $\mathrm{Shift}(\mu f)$, $\mu \in \mathbb{C}$, тоже конечномерны.

Из этиъ задач вытекает, что для любого экспоненциального многочлена f пространство $\mathrm{Shift}(f)$ конечномерно. Оказывается, верно и обратное, см., например[15].

Теорема. *Пространство* $\mathrm{Shift}(f)$ *в том и только том случае конечномерно, когда* f *является экспоненциальным многочленом.*

3. Характеризация многочленов. Пусть $f \in \mathbb{R}^{\mathbb{R}}$. Обозначим через $\mathrm{HShift}(f)$ подпространство, порожденное всеми сдвигами функции f:

$$\mathrm{HShift}(f) = \langle H_b T_a f, a \in \mathbb{R}, b \in \mathbb{R}^* \rangle.$$

Совсем просто доказать следующий результат, см., например[16].

Теорема. *Пространство* $\mathrm{HShift}(f)$ *в том и только том случае конечномерно, когда* f *является многочленом.*

---

[15] P.G.Laird, On characterizations of exponential polynomials. — Pacif. J. Math., 1979, vol.80, p.503–507.

[16] P.G.Laird, R.McCann, On some characterizations of polynomials. — Amer. Math. Monthly, 1984, vol.91, N.2, p.114–116.

§ 8♠. Интересные примеры линейной зависимости

1. Периодические функции. К линейной зависимости сводятся многие вопросы, где априори это не сразу понятно. Вот типичный пример использования идеи линейной зависимости, на роль которого в астрономии и механике обратил внимание А.Пуанкаре.

Задача. Когда сумма двух периодических функций $\mathbb{R} \longrightarrow \mathbb{R}$ является периодической функцией?

Решение. Пусть периоды функции f и g равны α и β, соответственно. Если отношение α/β рационально, то α и β линейно зависимы над $\mathbb{Z}$ и, следовательно, существует $\omega \in \mathbb{R}$ такое, что $\alpha, \beta \in \mathbb{Z}\omega$. Тогда $f+g$ будет периодической функцией с периодом ω. Если же $\alpha/\beta \notin \mathbb{Q}$, т.е. α и β линейно независимы над $\mathbb{Z}$, то в множестве $m\alpha + n\beta > 0$, $m, n \in \mathbb{Z}$, нет наименьшего элемента, так что функция $f+g$ не может быть периодической.

Мы вернемся к следующей теме в Главах IV и ?.

Задача. Рассмотрим пространство V функций $\mathbb{R} \longrightarrow \mathbb{R}$, порожденное сдвигами функции sin, т.е. всеми функциями вида $x \mapsto \sin(x+y)$, $y \in \mathbb{R}$. Показать, что в действительности это пространство двумерно и в качестве его базиса можно взять, например, функции sin и cos. Напомним, что $\cos(x) = \sin(x + \pi/2)$ действительно лежит в V.

2. Теорема Безиковича. Сейчас мы приведем еще один кажнейший пример линейной независимой системы. Трагическое открытие пифагорейцев состояло в том, что 1 и $\sqrt{2}$ линейно независимы над $\mathbb{Q}$. В школе Вам наверняка предлагали доказывать иррациональность чисел $\sqrt{2}+\sqrt{3}$ или $\sqrt{2}+\sqrt{3}+\sqrt{5}$.

Задача. Докажите, что $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ линейно независимы над $\mathbb{Q}$.

Эта задача допускает следующее классическое обобщение.

Теорема Безиковича. *Пусть $p_1, \ldots, p_2$ — попарно различные простые, тогда семейство*

$$\sqrt[n]{p_1^{m_1} \ldots p_s^{m_2}}, \qquad 0 \leq m_i < n,$$

линейно независимо над $\mathbb{Q}$.

Задача. Докажите, что $\ln(p)$, $p \in \mathbb{P}$ линейно независимы над $\mathbb{Q}$.

Решение. Это основная теорема арифметики целых чисел.

3. Теорема Линдеманна—Вейерштрасса. Следующая замечательная классическая теорема[17] представляет собой один из важнейших результатов теории трансцендентных чисел. Напомним, что через $\overline{\mathbb{Q}}$ обозначается поле алгебраических чисел.

Теорема Линдеманна—Вейерштрасса. *Для любых попарно различных алгебраических чисел $\lambda_1, \ldots, \lambda_n \in \overline{\mathbb{Q}}$ числа $e^{\lambda_1}, \ldots, e^{\lambda_n}$ линейно независимы над $\overline{\mathbb{Q}}$.*

Заметим, что в § ? мы приведем совсем простое доказательство того, что *функции* $x \mapsto e^{\lambda_1 x}, \ldots, x \mapsto e^{\lambda_n x}$ линейно независимы, даже над $\mathbb{R}$. Здесь, однако, утверждается нечто совершенно другое и гораздо более сильное и удивительное, а именно, что линейно независимы уже *значения* этих функций в 1!

Вот еще одна задача, использующая идею линейной зависимости. Заметим, что алгебра A здесь не предполагается коммутативной. В действительности, самые важные приложения этого свойства относятся к

[17]K.Weierstrass, Zu Lindemann's Abhandlung "Über die Ludolph'sche Zahl". — Sitzungsberichte Preuss. Akad. Wiss., 1885, S.1067–1085 (Werke II, S.341–362).

§ 9♠. Теорема Дедекинда—Артина

Сейчас мы научимся доказывать линейную независимость различных интересных семейств функций над полем таких, например, как экспоненциальные мономы.

Пусть M — мультипликативный моноид, T — тело. Ненулевой гомоморфизм $\phi : M \longrightarrow T^{\times}$ называется **одномерным характером** M со значениями в T. Поскольку никаких других характеров у нас пока встречаться не будет, мы будем опускать здесь эпитет **одномерным** и называть ϕ просто **характером**. Пример: $x \mapsto 1$ представляет собой характер моноида M, называемый **тривиальным** или **главным** характером.

Ключом ко всем результатам настоящего параграфа является следующая простая лемма.

Лемма о характерах. *Пусть $\phi_1, \dots, \phi_n$ —характеры моноида M со значениями в теле T. Если $\phi_1, \dots, \phi_n$ линейно независимы над T в T^M и их линейная комбинация $\phi = \lambda_1\phi_1 + \ldots + \lambda_n\phi_n$, $\lambda_i \in T$, тоже является характером, то ϕ сопряжен в T^* с тем ϕ_i, для которого $\lambda_i \neq 0$.*

Доказательство. Пусть $x, y \in M$. Вычислим $\phi(xy) = \phi(x)\phi(y)$ двумя способами. С одной стороны, $\phi(xy) = \sum \lambda_i\phi_i(xy) = \sum \lambda_i\phi_i(x)\phi_i(y)$. С другой стороны, $\phi(x)\phi(y) = \sum \phi(x)\lambda_i\phi_i(y)$. Так как это верно для всех $y \in M$, то $\sum \lambda_i\phi_i(x)\phi_i = \sum \phi(x)\lambda_i\phi_i$. Но ведь по предположению ϕ_i линейно независимы. Это значит, что $\lambda_i\phi_i(x) = \phi(x)\lambda_i$. Если $\lambda_i \neq 0$, отсюда вытекает, что $\phi = \lambda_i\phi_i\lambda_i^{-1}$, как и утверждалось.

Теорема Дедекинда—Артина. *Пусть K — поле, а ϕ_i — семейство попарно различных характеров моноида M со значениями в K. Тогда ϕ_i, $i \in I$, линейно независимы над K в K^M.*

Доказательство. Предположим, что ϕ_i, $i \in I$, линейно зависимы, тогда по лемме Дедекинда какие-то два из них сопряжены в K^* и, значит, равны.

Из этого незатейливого наблюдения вытекает больше замечательных следствий, чем можно предположить. Приведем некоторые из них.

Следствие 1. *Функции $x \mapsto e^{cx}$, $c \in \mathbb{C}$, линейно независимы над $\mathbb{C}$ в пространстве $\mathbb{C}^{\mathbb{R}}$ комплекснозначных функций над $\mathbb{R}$.*

Следствие 2. *Отображения $K \longrightarrow K$, $x \mapsto x^n$, где $n \in \mathbb{N}_0$, являются единственными полиномиальными отображениями, удовлетворяющими функциональному уравнению $f(xy) = f(x)f(y)$.*

Следствие 3. *Пусть A — алгебра размерности n над полем K, а L/K — расширение полей. Тогда существует не более n различных K-гомоморфизмов $A \longrightarrow L$.*

§ 10♠. Топологические базисы

Мы только что доказали, что в *любом* векторном пространстве над полем есть базис. Между тем, те, кто интересуется анализом, наверняка слышали о существовании банаховых пространств **без базиса**. Но ведь банаховы пространства являются векторными пространствами над $\mathbb{R}$ или $\mathbb{C}$ и, следовательно, должны иметь базис! Дело в том, что аналитики обычно рассматривают векторные пространства снабженные топологией, и называют просто базисом то, что алгебраисты называют **топологическим базисом** или **базисом Шаудера**. В свою очередь, то что мы называем просто базисом, аналитики называют **алгебраическим базисом** или **базисом Гамеля**.

Базис Шаудера. Пусть V — банахово пространство. Система $(x_1, x_2, \dots)$ векторов $x_i \in V$ называется **базисом Шаудера** пространства V, если каждое $x \in V$ допускает *единственное* представление в виде

$$x = \sum_{i=1}^{\infty} \lambda_i x_i.$$

Это равенство обычно понимается в том смысле, что последовательность частичных сумм $\sum_{i=1}^{n} \lambda_i x_i$ **сходится к** x **в смысле нормы**, т.е.

$$\lim_{n\to\infty} |x - \sum_{i=1}^{n} \lambda_i x_i| = 0.$$

Таким образом, бесконечный базис Шаудера **не является базисом** в нашем смысле: вектор не *представляется* как линейная комбинация базисных векторов, а всего лишь с любой точностью **аппроксимируется** такими линейными комбинациями. Все сепарабельные пространства, реально возникавшие в анализе, имели базис Шаудера, но в 1973 году шведский аналитик Пер Энфло построил контр-пример к классической гипетезе, утверждавшей что в любом сепарабельном банаховом пространстве существует базис Шаудера.

Стандартный базис пространств последовательностей. Чтобы показать, что понятие базиса Шаудера самым существенным образом зависит от топологии, покажем, что одна и та же система векторов может быть базисом большого количества различных пространств. Разумеется, для алгебраических базисов такое невозможно.

А именно, рассмотрим последовательности $e_j = (\delta_{ij})_{i\in\mathbb{N}}$, $j \in \mathbb{N}$, имеющие 1 на месте j и 0 на всех остальных местах. Тогда $(e_1, e_2, \dots)$ образует базис Шаудера в каждом из пространств l^p, $1 \le p < \infty$, а также в пространстве l^∞ последовательностей, сходящихся к 0.

Глава 5. ЛИНЕЙНЫЕ ОТОБРАЖЕНИЯ

— Ваша правда, мессер Бальдассаре, — согласился Моро. — Сколько раз говорил я ему: брось ты свою философию! Ну, да ведь знаете, такой уж народ художники. Ничего не поделаешь. С них и требовать нельзя.

Дмитрий Сергеевич Мережковский, *Воскресшие боги*

В этой главе мы *начинаем* изучать линейные отображения. Здесь мы делаем лишь самые первые шаги в этом направлении, фактически значительные фрагменты частей 2 и 3 посвящены именно более детальному изучению линейных отображений, их инвариантов и канонических форм.

Настоящая глава четко разбивается на две половины. В §§ 1 – 7 мы вводим несколько важнейших общих конструкций, связанных с матрицей линейного отображения. Здесь доказывается, что между свободными модулями конечного ранга над коммутативным кольцом не существует никаких линейных отображений, кроме умножения на матрицу. Эти конструкции постоянно используются в дальнейшем и в следующей главе мы вернемся к ней для изучения матриц.

С другой стороны, в §§ 8 – 14 мы обсуждаем основные понятия, связанные с коммутативными диаграммами и точными последовательностями, т. е. те свойства, которые выражаются в терминах композиции линейных отображений = произведения матриц. Кроме того, здесь мы доказываем некоторые простейшие общие факты. Эти факты было бы естественно рассматривать как простейшие утверждения о линейных отображениях, если бы не то обстоятельство, что — как это ни удивительно! — они *никогда* не излагаются в учебниках линейной алгебры. Обычно их можно найти только в первых параграфах книг по гомологической алгебре, в связи с диаграммным поиском[18].

§ 1♢. Структура модуля на $\mathrm{Hom}_R(U, V)$

Diese werden von rechts nach links geschrieben und gelesen und werden teilweise untereinander verbunden, teilweise unverbunden gelassen. — Они пишутся и читаются справа налево и в некоторых случаях образуют композицию, а в других оставляются как есть.

Brockelmann, *Arabische Grammatik*

[18]В настоящем издании последние два параграфа, 3×3-лемма и лемма о змее, маркированные ♣, опущены, как слишком технические. На матмехе доказательства этих результатов обычно включаются только в специальные курсы для студентов, обучающихся на кафедре высшей алгебры и теории чисел.

1. Сумма линейных отображений. Пусть R — произвольное кольцо с 1. Пусть, далее, $\phi, \psi : U \longrightarrow V$ линейные отображения с общей областью определения и общей областью значений, где оба U и V одновременно являются левыми или правыми R-модулями. Тогда сумма $\phi + \psi : U \longrightarrow V$, $x \mapsto \phi(x) + \psi(x)$, этих линейных отображений тоже является линейным отображением. Аддитивность $\phi + \psi$ проверяется непосредственно

$$(\phi + \psi)(u + v) = \phi(u + v) + \psi(u + v) = \phi(u) + \phi(v) + \psi(u) + \psi(v) = \\ \phi(u) + \psi(v) + \phi(u) + \psi(v) = (\phi + \psi)(u) + (\phi + \psi)(v),$$

а однородность еще проще

$$(\phi + \psi)(u\lambda) = \phi(u\lambda) + \psi(u\lambda) = \phi(u)\lambda + \psi(u)\lambda = (\phi + \psi)(u)\lambda.$$

В силу поточечного характера эта операция обладает всеми свойствами сложения в V и превращает $\mathrm{Hom}_R(U, V)$ в абелеву группу.

Если правые R-модули U и V не несут никакой дополнительной структуры, абелеву группу $\mathrm{Hom}_R(U, V)$ нельзя естественно превратить в R-модуль. Для того, чтобы разумным образом задать умножение на скаляры, необходимо, чтобы хотя бы один из модулей U или V являлся *бимодулем*.

2. Структура левого модуля на $\mathrm{Hom}_R(U, V)$**.** Пусть как обычно U правый R-модуль, а V является S-модулем-R. Мы можем определить на $\mathrm{Hom}_R(U, V)$ умножение на скаляры *слева*, полагая

$$(\lambda\phi)(x) = \lambda(\phi(x)), \qquad \lambda \in S,\ \phi \in \mathrm{Hom}_R(U, V),\ x \in U.$$

В самом деле, следующая выкладка показывает, что так определенное отображение $\lambda\phi : U \longrightarrow V$ аддитивно:

$$(\lambda\phi)(x + y) = \lambda(\phi(x + y)) = \lambda(\phi(x) + \phi(y)) = \\ \lambda(\phi(x)) + \lambda(\phi(y)) = (\lambda\phi)(x) + (\lambda\phi)(y),$$

Проверка однородности совершенно аналогична:

$$(\lambda\phi)(x\alpha) = \lambda(\phi(x\alpha)) = \lambda(\phi(x)\alpha) = (\lambda(\phi(x)))\alpha = ((\lambda\phi)(x))\alpha.$$

В этих вычислениях мы ставим слишком много скобок, поэтому они выглядят почти столь же коряво и заскорузло, как программы на `Lisp`. Чтобы избежать этого в дальнейшем, мы будем — в соответствии с практикой `Mathematica` и `Maple` — считать, что независимо от порядка записи применение функции имеет более высокий приоритет, чем любая арифметическая операция. Таким образом, $\lambda\phi(x)$ истолковывается как $\lambda(\phi(x))$, а не как $(\lambda\phi)(x)$.

Теорема RL. *Относительно введенных операций* $\mathrm{Hom}_R(U_R, {}_SV_R)$ *является левым* S*-модулем.*

Доказательство. Все аксиомы модуля проверяются непосредственно по определению. Для полноты один раз приведем все детали. В дальнейшем проведение подобных выкладок будет оставляться читателю. Внешняя ассоциативность:

$$((\lambda\mu)\phi)(x) = (\lambda\mu)\phi(x) = \lambda(\mu\phi(x)) = \lambda((\mu\phi)(x)) = (\lambda(\mu\phi))(x).$$

Дистрибутивность относительно сложения скаляров:

$$((\lambda+\mu)\phi)(x) = (\lambda+\mu)\phi(x) = \lambda\phi(x) + \mu\phi(x) = \\ (\lambda\phi)(x) + (\mu\phi)(x) = (\lambda\phi+\mu\phi)(x).$$

Дистрибутивность относительно сложения векторов:

$$(\lambda(\phi+\psi))(x) = \lambda(\phi+\psi)(x) = \lambda(\phi(x)+\psi(x)) = \\ \lambda\phi(x) + \lambda\psi(x) = (\lambda\phi)(x) + (\lambda\psi)(x) = (\lambda\phi+\lambda\psi)(x).$$

Наконец, унитальность: $(1\phi)(x) = 1\phi(x) = \phi(x)$.

3. Структура правого модуля на $\mathrm{Hom}_R(U,V)$**.** Пусть как обычно V правый R-модуль, а U является S-модулем-R. Мы можем определить на $\mathrm{Hom}_R(U,V)$ умножение на скаляры *справа*, полагая

$$(\phi\lambda)(x) = \phi(\lambda x), \qquad \phi\in\mathrm{Hom}_R(U,V),\ \lambda\in S,\ x\in U.$$

Проверим, что так определенное отображение $\phi\lambda : U \longrightarrow V$ действительно линейно. Аддитивность:

$$(\phi\lambda)(x+y) = \phi(\lambda(x+y)) = \phi(\lambda x+\lambda y) = \\ \phi(\lambda x) + \phi(\lambda y) = (\phi\lambda)(x) + (\phi\lambda)(y).$$

Однородность:

$$(\phi\lambda)(x\alpha) = \phi(\lambda(x\alpha)) = \phi((\lambda x)\alpha) = \phi(\lambda x)\alpha = (\phi\lambda)(x)\alpha.$$

Теперь мы можем сформулировать аналог

Теорема RR. *Относительно введенных операций* $\mathrm{Hom}_R({}_SU_R, V_R)$ *является правым* S*-модулем.*

Обратите внимание на отличие этой теоремы от предыдущей, если раньше структура левого S-модуля на V задавала структуру левого же S-модуля на $\mathrm{Hom}(U,V)$, то теперь структура *левого* S-модуля на V задает структуру *правого* S-модуля на $\mathrm{Hom}(U,V)$. Это является еще одним выражением того принципа, что функтор $(U, V) \rightsquigarrow \mathrm{Hom}(U, V)$ ковариантен по второму аргументу и контравариантен по первому аргументу.

4. Гомоморфизмы левых модулей. Пусть теперь U и V два левых R-модуля. Если V является R-модулем-S, то мы можем определить на $\mathrm{Hom}_R(U, V)$ умножение на скаляры *справа*, полагая

$$(x)(\phi\lambda) = ((x)\phi)\lambda, \qquad x \in U,\ \phi \in \mathrm{Hom}_R(U, V),\ \lambda \in S.$$

Если U является R-модулем-S, то мы можем определить на $\mathrm{Hom}_R(U, V)$ умножение на скаляры *слева*, полагая

$$(x)(\lambda\phi) = (x\lambda)\phi, \qquad x \in U,\ \lambda \in S,\ \phi \in \mathrm{Hom}_R(U, V).$$

Проверка линейности так определенных отображений, как и доказательство следующих результатов оставляется читателю. Мы настоятельно рекомендуем начинающему фактически произвести все эти проверки, для того, чтобы попрактиковаться в использовании аксиом и освоиться с записью функции справа от аргумента!

Теорема LR. *Относительно введенных операций* $\mathrm{Hom}_R({}_RU, {}_RV_S)$ *является правым* S*-модулем.*

Теорема LL. *Относительно введенных операций* $\mathrm{Hom}_R({}_RU_S, {}_RV)$ *является левым* S*-модулем.*

Обратите внимание, что снова задание правой структуры на втором аргументе Hom порождает правую же структуру на $\mathrm{Hom}(U, V)$, но задание *правой* структуры на первом аргументе ведет к *левой* структуре на $\mathrm{Hom}(U, V)$.

5. Случай коммутативного кольца. В случае, когда кольцо R коммутативно каждый модуль можно рассматривать как R-модуль-R. Таким образом, в этом случае $\mathrm{Hom}_R(U, V)$ естественно снабжается структурой R-модуля любым из четырех описанных выше способов.

§ 2$\diamondsuit$. Структура алгебры на $\mathrm{End}_R(U)$

Очевидно, что композиция линейных отображений снова линейна. В самом деле, пусть $\phi : U \longrightarrow V$ и $\psi : V \longrightarrow W$ суть два линейных отображения. Непосредственное вычисление показывает, что композиция аддитивна,

$$(\psi\phi)(u + v) = \psi(\phi(u + v)) = \psi(\phi(u) + \phi(v)) = \\ \psi(\phi(u)) + \psi(\phi(v)) = (\psi\phi)(u) + (\psi\phi)(v).$$

Точно так же проверяется и однородность,

$$(\psi\phi)(u\lambda) = \psi(\phi(u\lambda)) = \psi(\phi(u)\lambda) = \psi(\phi(u))\lambda = (\psi\phi)(u)\lambda.$$

Таким образом, композиция задает следующую операцию на группах Hom:

$$\mathrm{Hom}(V,W)\times\mathrm{Hom}(U,V)\longrightarrow\mathrm{Hom}(U,W)$$

Необычный порядок сомножителей в левой части связан, конечно, с тем, что мы записываем отображения так, как это принято в теории множеств, слева от аргумента и, следовательно, компонуем их справа налево.

Следующий результат показывает, что композиция дистрибутивна относительно сложения.

Предложение. *Пусть* $\phi,\psi\in\mathrm{Hom}(V,W)$, *а* $\theta,\eta\in\mathrm{Hom}(U,V)$. *Тогда*

$$(\phi+\psi)\theta=\phi\theta+\psi\theta,\qquad \phi(\theta+\eta)=\phi\theta+\phi\eta.$$

Доказательство. В самом деле,

$$((\phi+\psi)\theta)(u)=(\phi+\psi)\theta(u)=\phi(\theta(u))+\psi(\theta(u))=(\phi\theta)(u)+(\psi\theta)(u).$$

С другой стороны,

$$(\phi(\theta+\eta))(u)=\phi((\theta+\eta)(u))=\phi(\theta(a)+\eta(a))=\\ \phi(\theta(a))+\phi(\eta(a))=(\phi\theta)(a)+(\phi\eta)(a).$$

Обратите внимание на принципиальное отличие второй выкладки от первой. При доказательстве левой дистрибутивности мы пользовались только определением композиции и суммы двух отображений в абелеву группу, поэтому левая дистрибутивность композиции относительно сложения имеет место для любых отображений, не обязательно даже линейных В то же время при доказательстве правой дистрибутивности мы явным образом пользовались линейностью ϕ

Теорема. *Множество* $\mathrm{End}_R(U)$ *является ассоциативным кольцом с 1 относительно сложения и композиции эндоморфизмов. Применение эндоморфизма к вектору превращает правый/левый* R*-модуль* U *в левый/правый* $\mathrm{End}_R(U)$*-модуль.*

§ 3♠. Функториальность

В настоящем параграфе мы покажем, что Hom_R можно рассматривать как *функтор* от двух аргументов

$$U,V\rightsquigarrow\mathrm{Hom}_R(U,V),$$

причем этот функтор обладает очень хорошими свойствами.

Пусть $\phi:Z\longrightarrow U$, $\psi:V\longrightarrow W$ линейные отображения. Тогда естественно определяется гомоморфизм

$$\mathrm{Hom}(\phi,\psi):\mathrm{Hom}(U,V)\longrightarrow\mathrm{Hom}(Z,W).$$

А именно, гомоморфизм $\mathrm{Hom}(\phi,\psi)$ сопоставляет каждому линейному отображению $\theta : U \longrightarrow V$ композицию $\psi\theta\phi : Z \longrightarrow W$. Таким образом,

$$\mathrm{Hom}(\phi,\psi)(\theta) = \psi\theta\phi.$$

Обратите внимание на то, что функтор Hom **ковариантен** по второму аргументу в том смысле, что линейное отображение $\psi : V \longrightarrow W$ порождает линейное отображение

$$\mathrm{Hom}(U,\psi) : \mathrm{Hom}(U,V) \longrightarrow \mathrm{Hom}(U,W),$$

действующее *в том же направлении.* В то же время, этот функтор **контравариантен** по первому аргументу, иными словами, линейное отображение $\phi : Z \longrightarrow U$ порождает линейное отображение

$$\mathrm{Hom}(\phi,V) : \mathrm{Hom}(U,V) \longrightarrow \mathrm{Hom}(Z,V),$$

действующее *в противоположном направлении.*

Теорема. *Гомоморфизм* Hom *обладает следующими свойствами*

- $\mathrm{Hom}(\phi\phi',\psi'\psi) = \mathrm{Hom}(\phi',\psi')\,\mathrm{Hom}(\phi,\psi)$.
- $\mathrm{Hom}(\mathrm{id}_U,\mathrm{id}_V) = \mathrm{id}_{\mathrm{Hom}(U,V)}$.
- $\mathrm{Hom}(\phi+\phi',\psi) = \mathrm{Hom}(\phi,\psi) + \mathrm{Hom}(\phi',\psi)$.
- $\mathrm{Hom}(\phi,\psi+\psi') = \mathrm{Hom}(\phi,\psi) + \mathrm{Hom}(\phi,\psi')$.

Доказательство. Первая формула представляет собой еще один вариант ассоциативности композиции:

$$\mathrm{Hom}(\phi\phi',\psi\psi')(\theta) = \psi'\psi\theta\phi\phi' = \\ \mathrm{Hom}(\phi',\psi')(\psi\theta\phi) = \mathrm{Hom}(\phi',\psi')\,\mathrm{Hom}(\phi,\psi)(\theta).$$

Вторая формула очевидна, а третья и четвертая были фактически доказаны в предыдущем параграфе.

§ 4♢. Матрица линейного отображения

Пусть U и V — два свободных R модуля, $u_1,\ldots,u_n$ — базис в U, а $v_1,\ldots,v_m$ — базис в V. В настоящем параграфе мы построим базис в модуле линейных отображений $\mathrm{Hom}(U,V)$. Определим линейное отображение $\phi_{ij} : U \longrightarrow V$ следующей формулой

$$\phi_{ij}(u_h) = \begin{cases} 0, & h \neq j, \\ v_i, & h = j. \end{cases}$$

Теорема. *Линейные отображения*

$$\phi_{ij}, \qquad 1 \leq i \leq m,\ 1 \leq j \leq n,$$

образуют базис R-модуля $\mathrm{Hom}(U, V)$.

Доказательство. Докажем прежде всего, что ϕ_{ij} линейно независимы. В самом деле, пусть $\sum \lambda_{ij}\phi_{ij} = 0$ линейная зависимость между ними. Тогда для любого $h = 1, \ldots, n$ получаем

$$0 = \big(\sum \lambda_{ij}\phi_{ij}\big)(u_h) = \sum \lambda_{ij}\phi_{ij}(u_h) = \sum \lambda_{ih}v_i.$$

Так как $v_1, \ldots, v_m$ линейно независимы, то все $\lambda_{ih} = 0$.

Рассмотрим теперь произвольное линейное отображение $\phi \in \mathrm{Hom}(U, V)$. Тогда для любого $h = 1, \ldots, n$ образ $\phi(u_h) \in V$ раскладывается по базису $v_1, \ldots, v_m$ модуля V. Пусть $\phi(u_h) = a_{1h}v_1 + \ldots + a_{1h}v_h$. Докажем, что $\phi = \sum \lambda_{ij}\phi_{ij}$. Докажем, что тогда $\phi = \sum \lambda_{ij}\phi_{ij}$. В самом деле, в силу определения λ_{ih} для всех h имеет место равенство $\phi(u_h) = (\sum \lambda_{ij}\phi_{ij})(u_h)$. Так как $u_1, \ldots, u_n$ базис в U, то, тем самым, действительно $\phi = \sum \lambda_{ij}\phi_{ij}$.

Следствие. *Если а модули U и V свободные модули конечного ранга над коммутативным кольцом R, то* $\mathrm{Hom}(U, V)$ *тоже является свободным R-модулем, причем* $\mathrm{rk}(\mathrm{Hom}(U, V) = \mathrm{rk}(U)\,\mathrm{rk}(V)$.

Иными словами, это следствие утверждает, что для *правых* свободных модулей конечного ранга над коммутативным кольцом имеет место изоморфизм

$$\mathrm{Hom}(R^n, R^m) \cong M(m, n, R).$$

При этом изоморфизм можно истолковать следующим образом. Отождествим векторы $x \in R^n$ и $y \in R^m$ с их столбцами координат в стандартных базисах. Тогда каждое линейное отображение $\phi : R^n \longrightarrow R^m$ есть умножение *слева* на некоторую матрицу $a \in M(m, n, R)$. Иными словами, $\phi(x) = ax$ для всех $x \in R^n$. Эта матрица a и есть матрица линейного отображения ϕ в стандартных базисах:

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = a \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Иногда матрица коэффициентов линейного отображения относительно базиса ϕ_{ij} обозначается через $a = {}_v[\phi]_u$. Ее можно истолковать следующим образом. Как видно их описанной выше интерпретации, столбцами матрицы a являются столбцы координат векторов $\phi(u_1), \ldots, \phi(u_n)$.

Разумеется, линейные отображения *левых* свободных модулей допускают аналогичную интерпретацию, при этом

$$\mathrm{Hom}({}^nR, {}^mR) \cong M(n, m, R),$$

а именно матрице $a \in M(n, m, R)$ соответствует линейное отображение $\phi : {}^nR \longrightarrow {}^mR$, $x \mapsto xa$ состоящее в умножении строки $x \in {}^nR$ на матрицу a *справа*.

§ 5 ♢. Преобразование матрицы линейного отображения

> The difference between an introvert and extrovert mathematicians is:
> An introvert mathematician looks at her shoes while talking to you.
> An extrovert mathematician looks at your shoes.
>
> Carl Gustav Jung

Пусть теперь $\phi : U \longrightarrow V$ — отображение одного свободного модуля в другой. Чтобы не загромождать обозначения дополнительными индексами, мы будем считать, что ранг модулей U и V определен однозначно. Пусть, скажем, $\mathrm{rk}(U) = n$, а $\mathrm{rk}(V) = m$. Выберем в модулях U и V базисы $u_1, \ldots, u_n$ и $v_1, \ldots, v_m$, соответственно и пусть $a = {}_v[\phi]_u$ — матрица линейного отображения ϕ в базисах u, v.

Заменим теперь базис $u_1, \ldots, u_n$ на $u'_1, \ldots, u'_n$, а базис $v_1, \ldots, v_m$ на $v'_1, \ldots, v'_m$. Что происходит при этом с матрицей отображения ϕ, как матрица $b = {}_{v'}[\phi]_{u'}$ выражается через матрицу a?

Сравнивая полученную в предыдущем параграфе формулу

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = a \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \qquad \begin{pmatrix} y'_1 \\ \vdots \\ y'_m \end{pmatrix} = b \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix},$$

выражающую координаты $\phi(x)$ в базисах v и v', соответственно, через координаты вектора x в базисах u и u', соответственно, с формулами преобразования координат

$$\begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = (u \rightsquigarrow u')^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \qquad \begin{pmatrix} y'_1 \\ \vdots \\ y'_m \end{pmatrix} = (v \rightsquigarrow v')^{-1} \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix},$$

мы видим, что

$$b \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = \begin{pmatrix} y'_1 \\ \vdots \\ y'_m \end{pmatrix} = (v \rightsquigarrow v')^{-1} \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} =$$

$$(v \rightsquigarrow v')^{-1} a \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (v \rightsquigarrow v')^{-1} a (u \rightsquigarrow u') \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}.$$

Сравнивая два выражения для координат образа, мы получаем

$$b = (v \rightsquigarrow v')^{-1} a (u \rightsquigarrow u'),$$

как и утверждалось.

§ 6 ♢. Линейные отображения прямых сумм

В настоящем параграфе мы обсудим чуть более общий подход к понятию матрицы линейного отображения. А именно, мы определим матрицу линейного отображения

$$\phi : U_1 \oplus \ldots \oplus U_n \longrightarrow V_1 \oplus \ldots \oplus V_m.$$

Заметим, что так как мы пишем операторы *слева*, нам придется записывать элементы прямых сумм как *столбцы* с компонентами из слагаемых, а вовсе не как сторчки, как это обычно принято!

Чтобы не обременять обозначения, рассмотрим случай $m = n = 2$, очевидное обобщение на произвольные m и n предоставляется студенту. Начнем с двух простейших частных случаев.

• Пусть вначале $n = 2$, $m = 1$. Тогда каждое линейное отображение $\phi : U \oplus V \longrightarrow W$ имеет вид $\phi = (\alpha, \beta)$, где $\alpha : U \longrightarrow W$, $\beta : V \longrightarrow W$, причем

$$(\alpha, \beta) \begin{pmatrix} u \\ v \end{pmatrix} = \alpha(u) + \beta(v).$$

Таким образом, мы установили следующий изоморфизм:

$$\mathrm{Hom}(U \oplus V, W) = \mathrm{Hom}(U, W) \oplus \mathrm{Hom}(V, W).$$

• Пусть теперь $n = 1$, $m = 2$. Тогда каждое линейное отображение $\psi : U \longrightarrow V \oplus W$ имеет вид $\psi = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$, где $\gamma : U \longrightarrow V$, $\delta : V \longrightarrow W$, причем

$$\begin{pmatrix} \gamma \\ \delta \end{pmatrix} (u) = \begin{pmatrix} \gamma(u) \\ \delta(u) \end{pmatrix}.$$

Таким образом, мы установили следующий изоморфизм:

$$\mathrm{Hom}(U, V \oplus W) = \mathrm{Hom}(U, V) \oplus \mathrm{Hom}(U, W).$$

Совмещая эти два изоморфизма, мы видим, что

$$\mathrm{Hom}(U \oplus V, W \oplus Z) = \mathrm{Hom}(U, W) \oplus \mathrm{Hom}(U, Z) \oplus \mathrm{Hom}(V, W) \oplus \mathrm{Hom}(V, Z).$$

Иными словами, любое линейное отображение $\phi : U \oplus V \longrightarrow W \oplus Z$ можно описать матрицей

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} (\alpha, b) \\ (\gamma, \delta) \end{pmatrix} = \left(\begin{pmatrix} \alpha \\ \gamma \end{pmatrix}, \begin{pmatrix} \beta \\ \delta \end{pmatrix} \right),$$

где $\alpha \in \mathrm{Hom}(U, W)$, $\beta \in \mathrm{Hom}(U, Z)$, $\gamma \in \mathrm{Hom}(V, W)$, $\delta \in \mathrm{Hom}(V, Z)$. Действие этой матрицы на элементе $U \oplus V$ выглядит как обычное умножение на матрицу *слева*, с тем, конечно, что в данном случае умножение вектора x слева на линейное отображение ψ, это применение ψ к x:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} \alpha(u) + \beta(v) \\ \gamma(u) + \delta(v) \end{pmatrix}$$

§ 7♡. Полулинейные отображения

Во многих реально встречающихся примерах встречаются аддитивные, но не линейные отображения. Такие отображения не являются однородными в обычном смысле, при вынесении скалярного множителя выносится не сам исходный скаляр, а какой-то другой. Обычно этот новый скалярный множитель выражается через исходный следующим образом.

Пусть $f : R \longrightarrow S$ — гомоморфизм колец с 1, U — правый R-модуль, а V — правый S-модуль. Отображение $\phi : U \longrightarrow V$ называется **полулинейным** по отношению к f — или, для краткости, просто **f-полулинейным** отображением или **f-гомоморфизмом** — если оно аддитивно и удовлетворяет тождеству

$$\phi(u\lambda) = \phi(u)f(\lambda).$$

Фактически в большинстве приложений f является изоморфизмом.

• Особенно часто возникает случай, когда f — комплексное сопряжения $\mathbb{C} \longrightarrow \mathbb{C}$, $z \mapsto \overline{z}$. В этом случае $\phi(u\lambda) = u\overline{\lambda}$. Чаще всего, когда в элементарных книгах идет речь о полулинейных отображениях, имеется в виду именно эта ситуация.

• Предположим, что кольцо R некоммутативно. Тогда гомотетия $v \mapsto v\theta$ с нецентральным коэффициентом $\theta \in R$ не является линейным отображением свободного правого R-модуля R в себя. В то же время, в случае обратимого $\theta \in R^*$ это отображение полулинейно по отношению к сопряжению при помощи θ. В самом деле, $v \mapsto (v\lambda)\theta = (v\theta)(\theta^{-1}\lambda\theta)$.

• Пусть $f : R \longrightarrow R$ — автоморфизм кольца R. Тогда отображение $f : R^n \longrightarrow R^n$, сопоставляющее столбцу (x_i) столбец $(f(x_i))$, является f-полулинейным.

• Пусть $f : R \longrightarrow S$ и $g : S \longrightarrow T$ — два гомоморфизма колец. Рассмотрим R-модуль U, S-модуль V и T-модуль W и два отображения $\phi : U \longrightarrow V$ и $\psi : V \longrightarrow W$, полулинейных относительно f и g, соответственно. Тогда их композиция $\psi \circ \phi : U \longrightarrow W$ полулинейна относительно $g \circ f : R \longrightarrow T$. В частности, композиция двух отображений, полулинейных относительно комплексного сопряжения, линейна.

• Случай, когда f является изоморфизмом, особенно важен еще и потому, что при этом для любого биективного f-полулинейного отображения $\phi : U \longrightarrow V$ отображение $\phi^{-1} : V \longrightarrow U$ является f^{-1}-полулинейным.

• Пусть V — векторное пространство над полем K. *Биективное* отображение векторного пространства V на себя называется **коллинеацией**, если оно полулинейно по отношению к некоторому изоморфизму K. Из двух предыдущих примеров вытекает, что множество всех коллинеаций пространства V образует группу, обозначаемую $\Gamma\mathrm{L}(V)$ и называемую **группой коллинеаций**. В случае $V = K^n$ эта группа обычно обозначается $\Gamma\mathrm{L}(n, K)$.

§ 8♢. Диаграммы модулей и гомоморфизмов

1. Точные последовательности. Мы часто будем иметь дело с последовательным применением нескольких гомоморфизмов. Например, если $f : U \longrightarrow V$ и $g : V \longrightarrow W$ — два линейных отображения, то их композиция $g \circ f$ тоже является линейным отображением и мы обычно будем писать

$$U \xrightarrow{f} V \xrightarrow{g} W$$

и называть такую картинку **последовательностью** гомоморфизмов.

Для многих приложений особенно важен случай, когда $\mathrm{Ker}(g) = \mathrm{Im}(f)$.

• Последовательность называется **полуточной** в члене V, если $g \circ f = 0$ или, иными словами, если $\mathrm{Im}(f) \leq \mathrm{Ker}(g)$. В этом случае $g(f(u)) = 0$ для любого $u \in U$.

• Последовательность называется **точной** в члене V, если $g(v) = 0$ в том и только том случае, когда найдется такое $u \in U$, что $v = f(u)$ или, иными словами, когда $\mathrm{Ker}(g) = \mathrm{Im}(f)$.

Ясно, что точная последовательность полуточна, однако в действительности точность есть *гораздо* более сильное утверждение. А именно, требуется не только то, чтобы g отображало в 0 все приходящее из f, но и то, чтобы g не отображало в 0 *ничего лишнего*!!! Приведем два простейших примера такой ситуации:

• Для любого U существует единственный гомоморфизм $0 \longrightarrow U$, переводящий 0 в 0. Последовательность

$$0 \longrightarrow U \xrightarrow{f} V$$

в том и только том случае точна в члене U, когда f является мономорфизмом — в образе отображения $0 \longrightarrow U$ лежит только 0, так что только 0 лежит в ядре f.

• Для любого V существует единственный гомоморфизм $V \longrightarrow 0$, переводящий все в 0. Последовательность

$$U \xrightarrow{f} V \longrightarrow 0$$

в том и только том случае точна в члене V, когда f является эпиморфизмом — все элементы $v \in V$ лежат в ядре отображения $V \longrightarrow 0$, значит все они приходят из U.

В действительности, обычно мы будем иметь дело с более длинными последовательностями. Например, пусть

$$U_1 \xrightarrow{f_1} U_2 \xrightarrow{f_2} U_3 \xrightarrow{f_2} \dots \xrightarrow{f_n} U_{n+1}$$

последовательность, состоящая из n гомоморфизмов. Она называется **точной**, если она точна в *каждом* из членов $U_2, \dots, U_n$. Иными словами, предполагается, что для каждого $i = 1, \ldots, n-1$ имеет место равенство $\operatorname{Ker}(f_{i+1}) = \operatorname{Im}(f_i)$. Отметим важнейшие специальные случаи.

• Последовательность

$$0 \longrightarrow U \xrightarrow{\ f\ } V \xrightarrow{\ g\ } W \longrightarrow 0$$

в том и только том случае точна, когда U можно рассматривать как подмодуль в V, причем g уствнавливает измоморфизм $W \cong V/U$. В самом деле, как мы уже знаем, точность последовательности в члене U эквивалентна тому, что f является вложением, так что мы можем отождествить U с $f(U) \leq V$. Точность последовательности в члене W эквивалентна сюръективности g, т.е. тому, что $W = \operatorname{Im}(g)$. Наконец, точность в члене V как раз и означает, что $\operatorname{Ker}(g) = \operatorname{Im}(f) = U$. Но тогда по теореме о гомоморфизме $W = \operatorname{Im}(g) \cong V/\operatorname{Ker}(g) = V/U$.

• Любой гомоморфизм $f : U \longrightarrow V$ может быть включен в точную последовательность

$$0 \longrightarrow \operatorname{Ker}(f) \longrightarrow U \xrightarrow{\ f\ } V \longrightarrow \operatorname{Coker}(f) \longrightarrow 0$$

Часто в одной и той же диаграмме гомоморфизмы будут изображаться как в горизонтальном, так и в вертикальном направлении. В этом случае мы будем говорить о точных строках и точных столбцах.

2. Коммутативные диаграммы. В соответствии с общими соглашениями, которые мы обсуждали в Книге I, квадрат

$$\begin{tikzcd} U \arrow[r, "f"] \arrow[d, "h"'] & V \arrow[d, "k"] \\ W \arrow[r, "g"] & Z \end{tikzcd}$$

модулей и их гомоморфизмов, называется **коммутативным**, если $k \circ f = g \circ h$, иными словами, если для любого $u \in U$ имеет место равенство $k(f(u)) = g(h(u))$. Аналогично треугольник

$$\begin{tikzcd} U \arrow[r, "f"] & V \\ & W \end{tikzcd}$$

называется коммутативным, если $g = h \circ f$ или, иными словами, если для любого $u \in U$ имеет место равенство $g(u) = h(f(u))$.

В дальнейшем нам часто будут встречаться диаграммы, составленные из нескольких треугольников и квадратов. Такие диаграммы будут называться **коммутативными**, если *все* входящие в их состав треугольники и квадраты коммутативны.

Обычно коммутативность используется в сочетании с точностью и возможно еще какими-то утверждениями о гомоморфизмах. Например, утверждение о том, что следующая диаграмма коммутативна, а ее строки точны

$$\begin{tikzcd}
0 \arrow[r] & U\cap V \arrow[r] \arrow[d] & U \arrow[r] \arrow[d] & U/(U\cap V) \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & V \arrow[r] & U+V \arrow[r] & (U+V)/V \arrow[r] & 0
\end{tikzcd}$$

включает в себя как формулировку теоремы Нетер об изоморфизме, так и ее доказательство.

§ 9◊. Неравенства Фробениуса и Сильвестра

Мы продолжаем рассматривать ранги линейных отображений векторных пространств над полями. Пусть $\phi : U \longrightarrow V$ и $\psi : V \longrightarrow W$ суть два линейных отображения. Как ранг их композиции $\psi\phi : U \longrightarrow W$ связан с рангами самих отображений ϕ и ψ?

Прежде всего, совершенно очевидно, что $\mathrm{Im}(\psi\phi) \leq \mathrm{Im}(\psi)$ и, таким образом, $\mathrm{rk}(\psi\phi) \leq \mathrm{rk}(\psi)$. С другой стороны, так как $\mathrm{Im}(\psi\phi)$ является фактор-пространством $\mathrm{Im}(\phi)$, то $\mathrm{rk}(\psi\phi) \leq \mathrm{rk}(\phi)$. Таким образом, мы получаем следующую очевидную оценку $\mathrm{rk}(\psi\phi)$ сверху.

Утверждение. *Для любых линейных отображений*

$$U \xrightarrow{\ \phi\ } V \xrightarrow{\ \psi\ } W$$

выполняется неравенство

$$\mathrm{rk}(\psi\phi) \leq \min(\mathrm{rk}(\phi), \mathrm{rk}(\psi)).$$

Получить оценку $\mathrm{rk}(\psi\phi)$ снизу несколько сложнее.

Лемма. *Пусть*

$$U \xrightarrow{\ \phi\ } V \xrightarrow{\ \psi\ } W$$

суть два линейных отображения. Тогда

$$\dim(\mathrm{Ker}(\psi)\cap\mathrm{Im}(\phi)) + \dim(\mathrm{Im}(\psi\phi)) = \dim(\mathrm{Im}(\phi)).$$

Доказательство. Применяя к линейному отображению $\psi|_{\mathrm{Im}(\phi)}$ теорему о размерности ядра и образа, получим

$$\dim(\psi|_{\mathrm{Im}(\phi)}) + \dim(\psi|_{\mathrm{Im}(\phi)}) = \dim(\mathrm{Im}(\phi)).$$

Остается лишь заметить, что

$$\mathrm{Ker}(\psi|_{\mathrm{Im}(\phi)}) = \mathrm{Ker}(\psi)\cap\mathrm{Im}(\phi), \qquad \mathrm{Im}(\psi|_{\mathrm{Im}(\phi)}) = \mathrm{Im}(\psi\phi).$$

Теперь у нас все готово, чтобы доказать основное неравенство, связывающее ранги композиций.

Неравенство Фробениуса. *Пусть*

$$U \xrightarrow{\phi} V \xrightarrow{\psi} W \xrightarrow{\theta} Z$$

суть три линейных отображения. Тогда

$$\mathrm{rk}(\psi\phi) + \mathrm{rk}(\theta\psi) \leq \mathrm{rk}(\psi) + \mathrm{rk}(\theta\psi\phi).$$

Доказательство. Применяя лемму к парам отображений (ψ, θ) и $(\psi\phi, \theta)$ получим следующие равенства:

$$\dim(\mathrm{Ker}(\theta) \cap \mathrm{Im}(\psi)) + \dim(\mathrm{Im}(\theta\psi)) = \dim(\mathrm{Im}(\psi)),$$

$$\dim(\mathrm{Ker}(\theta) \cap \mathrm{Im}(\psi\phi)) + \dim(\mathrm{Im}(\theta\psi\phi)) = \dim(\mathrm{Im}(\psi\phi)).$$

С учетом этих равенств для доказательства теоремы остается лишь заметить, что так как $\mathrm{Im}(\psi\phi) \leq \mathrm{Im}(\psi)$, то

$$\mathrm{Ker}(\theta) \cap \mathrm{Im}(\psi\phi) \leq \mathrm{Ker}(\theta) \cap \mathrm{Im}(\psi)$$

и, в частности,

$$\dim(\mathrm{Ker}(\theta) \cap \mathrm{Im}(\psi\phi)) \leq \dim(\mathrm{Ker}(\theta) \cap \mathrm{Im}(\psi)).$$

Взяв в этом неравенстве $V = W$ и $\psi = \mathrm{id}_V$ мы получаем следующую оценку ранга $\mathrm{rk}(\psi\phi)$ снизу.

Неравенство Сильвестра. *Пусть*

$$U \xrightarrow{\phi} V \xrightarrow{\psi} W$$

суть два линейных отображения. Тогда

$$\mathrm{rk}(\psi\phi) \geq \mathrm{rk}(\phi) + \mathrm{rk}(\psi) - \dim(V).$$

§ 10♠. Фредгольмовы операторы

Линейное отображение $\phi : U \longrightarrow V$ одного векторного пространства в другое называется **фредгольмовым**, если его ядро $\mathrm{Ker}(\phi)$ имеет конечную размерность в U, а его образ $\mathrm{Im}(\phi)$ — конечную коразмерность в V. В функциональном анализе принято в этом случае говорить о **фредгольмовых операторах**. Разность

$$\mathrm{ind}(\phi) = \dim(\mathrm{Ker}(\phi)) - \mathrm{codim}(\mathrm{Im}(\phi))$$

называется **индексом** фредгольмова оператора ϕ. В анализе обычно рассматриваются фредгольмовы операторы между *топологическими* векторными пространствами и в этом случае в определение фредгольмова оператора часто включается *замкнутость* образа. Однако, это требование излишне, так как оно автоматически следует из того, что коразмерность образа конечна.

Теорема об индексе. *Произведение двух фредгольмовых операторов* $\phi : U \longrightarrow V$ *и* $\psi : V \longrightarrow W$ *является фредгольмовым оператором, причем*

$$\mathrm{ind}(\psi\phi) = \mathrm{ind}(\phi) + \mathrm{ind}(\psi).$$

Обычные доказательства этой теоремы используют замысловатые аналитические соображения. В действительности это чисто алгебраический результат, непосредственное следствие теоремы о размерности ядра и образа[19,20].

Доказательство. В случае конечномерных пространств

$$\begin{aligned}\mathrm{ind}(\phi) = \dim(\mathrm{Ker}(\phi)) - \mathrm{codim}(\mathrm{Im}(\phi)) = \\ \dim(\mathrm{Ker}(\phi)) - (\dim(V) - \dim(\mathrm{Im}(\phi))) = \\ (\dim(\mathrm{Ker}(\phi)) + \dim(\mathrm{Im}(\phi))) - \dim(V) = \dim(U) - \dim(V).\end{aligned}$$

Таким образом, в конечномерном случае теорема об индексе превращается в равенство

$$(\dim(U) - \dim(V)) + (\dim(V) - \dim(W)) = (\dim(U) - \dim(W)),$$

в которое верится сразу.

Оказывается, общий случай моментально сводится к конечномерному. Для этого мы сейчас построим такие разложения в прямую сумму

$$U = U_0 \oplus U_1, \qquad V = V_0 \oplus V_1, \qquad W = W_0 \oplus W_1,$$

что ограничения $\phi|_{U_1}$ и $\psi|_{V_1}$ определяют изоморфизмы $U_1 \cong V_1 \cong W_1$, а пространства U_0, V_0 и W_0 конечномерны и $\phi(U_0) \leq V_0$, $\psi(V_0) \leq W_0$. Ясно, что это как раз и сводит доказательство теоремы об индексе к случаю конечномерных пространств U_0, V_0, W_0.

В самом деле, пусть $U_0 = \phi^{-1}(\mathrm{Ker}(\psi))$ и U_1 — какое-то дополнение к U_0 в U. Так как U_0 конечномерно, то U_1 имеет конечную коразмерность в U. Это значит, что его образ $V_1 = \phi(U_1)$ имеет конечную коразмерность в пространстве $\phi(U)$, которое в свою очередь имеет конечную коразмерность в V. Так как $V_1 \cap \mathrm{Ker}(\psi) = 0$, то в V существует такое дополнение V_0 к V_1, которое содержит $\mathrm{Ker}(\psi)$. По той же причине, что и выше, $\psi(V_1)$ имеет конечную коразмерность в W, а так как $\mathrm{Ker}(\psi) \leq V_0$, то $W_1 \cap \psi(V_) = 0$, и, значит, в W существует такое дополнение W_0 к W_1, которое содержит $\psi(V_0)$.

[19] См., например, Р.Пале, Семинар по теореме Атьи—Зингера об индексе. М., Мир, 1970, 359с.

[20] D.Sarason, The multiplication theorem for Fredholm operators. — Amer. Math. Monthly, 1987, vol. , p.68-70.

§ 11♠. Лемма о трех гомоморфизмах

Следующее простое, но очень часто применяемое соображение показывает, как именно используются условия коммутативности и точности. Применяемые в доказательстве этой леммы соображения называются **диаграммным поиском** = `diagram chasing`.

Лемма о трех гомоморфизмах. *Пусть строки коммутативной диаграммы*

$$\begin{tikzcd} U_1 \arrow[r, "\phi_1"] \arrow[d, "\pi"] & U_2 \arrow[r, "\phi_2"] \arrow[d, "\rho"] & U_3 \arrow[d, "\sigma"] \\ V_1 \arrow[r, "\psi_1"] & V_2 \arrow[r, "\psi_2"] & V_3 \end{tikzcd}$$

являются точными последовательностями.

- *Если σ инъективно, то*

$$\mathrm{Im}(\rho)\cap\mathrm{Im}(\psi_1)=\mathrm{Im}(\psi_1\circ\pi)=\mathrm{Im}(\rho\circ\phi_1).$$

- *Если π сюръективно, то*

$$\mathrm{Ker}(\rho)+\mathrm{Im}(\phi_1)=\mathrm{Ker}(\psi_2\circ\rho)=\mathrm{Ker}(\sigma\circ\phi_2).$$

Доказательство. Включение

$$\mathrm{Im}(\psi_1\circ\pi)=\mathrm{Im}(\rho\circ\phi_1)\le\mathrm{Im}(\rho)\cap\mathrm{Im}(\psi_1)$$

очевидно. Гораздо интереснее, почему выполняется обратное включение! Возьмем $x\in\mathrm{Im}(\rho)\cap\mathrm{Im}(\psi_1)$. Так как $x\in\mathrm{Im}(\rho)$, то найдется элемент $y\in U_2$ такой, что $\rho(y)=x$. С другой стороны, так как $x\in\cap\,\mathrm{Im}(\psi_1)$, то в силу точности нижней строки имеем $\psi_2(x)=0$ и, значит, в силу коммутативности второго квадрата, $\sigma\circ\phi_2(y)=\psi_2\circ\sigma(y)=\psi_2(x)=0$. Отсюда в сиду инъективности σ следует, что $\phi_2(y)=0$. В силу точности первой строки найдется $z\in U_1$ такое, что $\phi_1(z)=y$. Но тогда $x=\rho(y)=\rho\circ\phi_1(z)\in\mathrm{Im}(\rho\circ\phi_1)$, как и утверждалось.

Перейдем теперь к доказательству второго равенства. Так как $\phi_2\circ\phi_1=0$, то из того, что $x\in\mathrm{Im}(\phi_1)$, следует, что $x\in\mathrm{Ker}(\phi_2)$ и, тем более, $x\in\mathrm{Ker}(\sigma\circ\phi_2)=\mathrm{Ker}(\psi_2\circ\rho)$. Ясно, что это включение справедливо и для $x\in\mathrm{Im}(\rho)$. Поэтому

$$\mathrm{Ker}(\rho)+\mathrm{Im}(\phi_1)\le\mathrm{Ker}(\psi_2\circ\rho)=\mathrm{Ker}(\sigma\circ\phi_2).$$

Обратно, пусть $x\in\mathrm{Ker}(\psi_2\circ\rho)$. Тогда $\rho(x)\in\mathrm{Ker}(\psi_2)$ и в силу точности второй строки найдется такое $y\in V_1$, что $\rho(x)=\psi_1(y)$. В силу сюръективности π это означает, что найдется такое $z\in U_1$, что $\pi(z)=y$. В силду коммутативности первого квадрата $\rho(x)=\psi_1(y)=\psi_1(\pi(z))=\rho(\phi_1(z))$, так что $\rho(x-\phi_1(z))=0$, так что $x=(x-\phi_1(z))+\phi_1(z)\in\mathrm{Ker}(\rho)+\mathrm{Im}(\phi_1)$, как и утверждалось.

§ 11♠. Лемма о пяти гомоморфизмах

Приведем еще один пример диаграммного поиска.

Лемма о пяти гомоморфизмах. *Пусть строки коммутативной диаграммы*

$$\begin{tikzcd}
U_{-2} \arrow[r, "\phi_{-2}"] \arrow[d, "\pi_{-2}"] & U_{-1} \arrow[r, "\phi_{-1}"] \arrow[d, "\pi_{-1}"] & U_0 \arrow[r, "\phi_0"] \arrow[d, "\pi_0"] & U_1 \arrow[r, "\phi_1"] \arrow[d, "\pi_1"] & U_2 \arrow[d, "\pi_2"] \\
V_{-2} \arrow[r, "\psi_{-2}"] & V_{-1} \arrow[r, "\psi_{-1}"] & V_0 \arrow[r, "\psi_0"] & V_1 \arrow[r, "\psi_1"] & V_2
\end{tikzcd}$$

являются точными последовательностями. Тогда если π_{-2} эпиморфно, а π_{-1} и π_1 мономорфны, то π_0 тоже мономорфно.

Доказательство. Пусть $x \in \operatorname{Ker}(h_0)$. В силу коммутативности третьего квадрата $\pi_1(\phi_0(x)) = \psi_0(\pi_0(x)) = 0$. Так как по условию $\operatorname{Ker}(\pi_1) = 0$, то $\phi_0(x) = 0$. В силу точности верхней строки в члене U_0 найдется такой элемент $y \in U_{-1}$, что $\phi_{-1}(y) = x$. В силу коммутативности второго квадрата $\psi_{-1}(\pi_{-1}(y)) = \pi_0(\phi_{-1}(y)) = \pi_0(x) = 0$, так что $\pi_{-1}(y) \in \operatorname{Ker}(\psi_{-1})$. В силу точности нижней строки в члене V_{-1} найдется такое $z \in V_{-2}$, что $\pi_{-1}(y) = \psi_{-2}(z)$. Но ведь по условию π_{-2} эпиморфно, так что найдется $w \in U_{-2}$ такое, что $\pi_{-2}(w) = z$. В силу коммутативности первого квадрата $\pi_{-1}(\phi_{-2}(w)) = \psi_{-2}(\pi_{-2}(w)) = \psi_{-2}(z) = \pi_{-1}(y)$. Так как по условию π_{-1} мономорфизм, то отсюда следует $\phi_{-2}(w) = y$. В силу точности верхней строки в члене U_{-1} отсюда следует, что $x = \phi_{-1}(y) = \phi_{-2}(\phi_{-1}(w)) = 0$, как и утверждалось.

Как всегда, утверждение, двойственное к любой теореме про отображения модулей, тоже является теоремой. Поэтому лемму о пяти гомоморфизмах можно сформулировать еще и так.

Лемма о пяти гомоморфизмах (bis). *Если в условиях предыдущей леммы π_2 мономорфно, а π_{-1} и π_1 эпиморфны, то π_0 тоже эпиморфно.*

Конечно, это утверждение сразу следует из предыдущего. Тем не менее, мы настоятельно рекомендуем начинающему самостоятельно провести диаграммный поиск в этом случае, чтобы убедиться, какие именно предположения об исходной диаграмме используются в доказательстве этого утверждения. Проделав это он убедится, что в доказательстве следствия использованы *все* условия.

Следствие. *Если в условиях леммы π_{-2} эпиморфно, π_2 мономорфно, а π_{-1} и π_1 изоморфизмы, то π_0 тоже изоморфизм.*

Следствие. *Пусть строки коммутативной диаграммы*

$$\begin{tikzcd}
0 \arrow[r] & U_1 \arrow[r] \arrow[d, "\pi"] & V_1 \arrow[r] \arrow[d, "\rho"] & W_1 \arrow[r] \arrow[d, "\sigma"] & 0 \\
0 \arrow[r] & U_2 \arrow[r] & V_2 \arrow[r] & W_2 \arrow[r] & 0
\end{tikzcd}$$

являются точными последовательностями. Тогда

- *Если* π *и* σ *мономорфизмы, то* ρ *тоже мономорфизм;*
- *Если* π *и* σ *эпиморфизмы, то* ρ *тоже эпиморфизм;*
- *Если* π *и* σ *изоморфизмы, то* ρ *тоже изоморфизм.*

Теперь читатель в состоянии самостоятельно доказать следующий результат, усиливающий лемму о пяти гомоморфизмах.

Лемма о четырех гомоморфизмах. *Предположим, что строки коммутативной диаграммы*

$$\begin{array}{ccccccc}
U_1 & \longrightarrow & U_2 & \xrightarrow{\phi} & U_3 & \longrightarrow & U_4 \\
\Big\downarrow{\scriptstyle \pi} & & \Big\downarrow{\scriptstyle \rho} & & \Big\downarrow{\scriptstyle \sigma} & & \Big\downarrow{\scriptstyle \tau} \\
V_1 & \longrightarrow & V_2 & \xrightarrow{\psi} & V_3 & \longrightarrow & V_4
\end{array}$$

являются точными последовательностями. Тогда если π *эпиморфизм, а* τ *мономорфизм, то*

- $\mathrm{Ker}(\sigma) = \phi(\mathrm{Ker}(\rho))$,
- $\mathrm{Im}(\rho) = \psi^{-1}(\mathrm{Im}(\sigma))$.

Глава 6. ДВОЙСТВЕННОСТЬ

Однажды Чжуану Чжоу приснилось, что он — бабочка, счастливая бабочка, достигшая исполнения желаний. Он наслаждался и не сознавал, что он — Чжоу. Но вдруг проснулся, удивился, что он — Чжоу, и долго не мог понять, то ли он Чжоу, которому снилось, что он бабочка, то ли он бабочка, которой снится, что она — Чжоу. А ведь Чжоу и бабочка — это совсем не одно и то же.

Чжуан-цзы

Приснилось однажды милиционеру, что он бабочка. Он весело порхал, делал ноздрями и не знал, что он милиционер, был счастлив. А проснувшись внезапно, даже удивился, что он совсем не бабочка, а милиционер. И он не знал уже, — милиционеру ли снилось, что он бабочка, или бабочке — что она милиционер.

Венедикт Ерофеев, *Из записных книжек*

Эх, Петька, Петька, — сказал Чапаев, — знавал я одного китайского коммуниста по имени Цзе Чжуан. Ему часто снился один сон — что он красная бабочка, летающая среди травы. И когда он просыпался, он часто не мог взять в толк, то ли это бабочке приснилось, что она занимается революционной работой, то ли это подпольщик видел сон, в котором он порхал среди цветов.

Виктор Пелевин, *Чапаев и Пустота*

Grand Master Turing once dreamed that he was a machine. When he awoke he exclaimed:
"I don't know whether I am Turing dreaming that I am a machine, or a machine dreaming that I am Turing!."

The Tao of Real Programming

Категории правых и левых модулей находятся в двойственности: каждому *правому* модулю можно сопоставить двойственный к нему *левый* модуль и наоборот. В случае проективных модулей конечного ранга, в частности, конечномерных векторных пространств, эти сопоставления взаимно обратны, строго говоря, именно этот факт обычно и называется двойственностью. В случае коммутативного основного кольца двойственность тесно связана с наличием скалярного произведения.

§ 1♢. Двойственный модуль

В настоящем параграфе мы сопоставим каждому правому/левому R-модулю левый/правый R-модуль линейных функционалов на нем.

Напомним, что **линейным функционалом** на V называется линейное отображение $\phi : V \longrightarrow R$,

$$\phi(u\alpha + v\beta) = \phi(u)\alpha + \phi(v)\beta.$$

Множество всех линейных функционалов на V обозначается через $V^* = \mathrm{Hom}(V, R)$ и называется **двойственным модулем**. Операции в V^* вводятся с

$$(\phi + \psi)(u) = \psi(u) + \psi(u), \qquad (\alpha\phi)(u) = \alpha\phi(u).$$

В случае векторных пространств V^* обычно называется **двойственным пространством**, а его элементы — **ковекторами**.

Отображение

$$V^* \times V \longrightarrow R, \qquad \phi, u \mapsto \phi(u),$$

называется каноническим спариванием между V^* и V. Однако, в этом обозначениии симметрия между ϕ и u нарушается гораздо сильнее, чем хотелось бы. В действительности, не только ϕ можно рассматривать как линейный функционал на V, но и u задает линейный функционал на V^*. Физики — и даже некоторые математики — вместо $\phi(u)$ обычно пишут что-нибудь в духе $\langle \phi \mid u \rangle$ или $\langle \phi, u \rangle$.

Теорема. *Если V свободный правый модуль конечного ранга с базисом $u_1, \ldots , u_n$, то V^* — свободный левый модуль с базисом $u_1^*, \ldots , u_n^*$, определенным равенствами*

$$u_i^*(u_j) = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}.$$

Построенный в теореме базис называется **двойственным базисом**. Он состоит из **координатных функций** по отношению к базису $u_1, \ldots , u_n$. А именно, если $x = \sum u_i x_i$, то u_i^* это в точности линейный функционал $x \mapsto x_i$, сопоставляющий вектору x его i-ю координату в базисе u.

Теорема означает, в частности, что если V свободный модуль конечного ранга, то $\mathrm{rk}(V^*) = \mathrm{rk}(V)$ и, *если не различать левые и правые модули*, то $V^* \cong V$. А именно, сопоставление $u_i \mapsto u_i^*$ продолжается до изоморфизма. Однако, этот изоморфизм не является каноническим, а зависит от выбора базиса $u_1, \ldots , u_n$.

§ 2♢. Преобразование координат ковектора

Империализму и всем реакционерам присуща двойственность — они одновременно являются и настоящими, и бумажными тиграми.

Мао Цзе-Дун

По самому определению двойственного базиса имеет место равенство

$$\begin{pmatrix} u_1^* \\ \vdots \\ u_n^* \end{pmatrix} (\, u_1, \ldots , u_n \,) = e.$$

Сопрягая его при помощи обратимой матрицы $g \in \mathrm{GL}(n, R)$, мы получим

$$g^{-1} \begin{pmatrix} u_1^* \\ \vdots \\ u_n^* \end{pmatrix} (\, u_1, \dots , u_n \,)\, g = g^{-1} e g = e.$$

Если $g = (u \rightsquigarrow v)$ матрица перехода от базиса u к базису v, то сравнивая это равенство с равенством

$$\begin{pmatrix} v_1^* \\ \vdots \\ v_n^* \end{pmatrix} (\, v_1, \dots , v_n \,) = e,$$

мы видим, что

$$\begin{pmatrix} v_1^* \\ \vdots \\ v_n^* \end{pmatrix} = g^{-1} \begin{pmatrix} u_1^* \\ \vdots \\ u_n^* \end{pmatrix}$$

Таким образом, двойственный базис преобразуется **контравариантно** по отношению к исходному базису.

Поскольку координаты в свою очередь преобразуются контравариантно по отношению к преобразованию базиса, это значит, что координаты ковектора по отношению к двойственному базису преобразуются **ковариантно** по отношению к исходному базису. Иными словами, если $(\alpha_1, \dots , \alpha_n)$ строка координат ковектора ϕ в базисе $u_1^*, \dots , u_n^*$, а $(\beta_1, \dots , \beta_n)$ — его строка координат в базисе $v_1^*, \dots , v_n^*$, а $g = (u \rightsquigarrow v)$ — матрица перехода от u к v, то

$$(\beta_1, \dots , \beta_n) = (\alpha_1, \dots , \alpha_n) g.$$

К сожалению, традиционные учебники линейной алгебры настаивают на том, чтобы для *коммутативного* кольца R записывать координаты в *левом* модуле V^* в виде столбца. При таком экстравагантном соглашении координаты в V^* будут преобразовываться по формуле

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = g^t \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix},$$

где транспонирование появляется ровно потому, что строка координат насильственно отформатирована в виде столбца.

Заметим, что если нам вдруг взбредет в голову записывать двойственный базис в виде строки, то при преобразовании двойственных базисов поверх образения тоже должно появиться транспонирование, так что

$$(v_1^*, \dots , v_n^*) = (u_1^*, \dots , u_n^*) g^{-t}.$$

Комментарий. Традиционно в геометрии и тензорном анализе V^* отождествляется с V посредством задания на V невырожденного скалярного произведения. В этом случае, чтобы подчеркнуть контравариантность по отношению к исходному базису, двойственный базис обычно обозначается через $e^1, \dots, e^n$. Координаты векторов пишутся соответственно. Так, когда $v \in V$ рассматривается как вектор, его координаты записываются с верхними индексами, $v = e_1 x^1 + \dots + e_n x^n$, а если он рассматривается как ковектор, то в виде $v = x_1 e^1 + \dots + x_n e^n$.

§ 3◇. Второе двойственное, двойственность

Образуем теперь двойственное пространство к двойственному пространству и запишем каноническое спаривание:

$$V^* \times V^{**} \longrightarrow R, \qquad \phi, \theta \mapsto (\phi)\theta.$$

Сопоставим вектору u функционал $\theta_u = u^{**} \in V^{**}$ полагая

$$(\phi)u^{**} = \phi(u), \qquad \phi \in V^*,$$

или, в компактной записи,

$$u \mapsto (u^{**} : \phi \mapsto \phi(u)).$$

Следующая теорема является одним из типичных проявлений явления известного как **двойственность**.

Теорема. *Если V свободный модуль конечного ранга, то отображение*

$$V \longrightarrow V^{**}, \qquad v \mapsto v^{**},$$

представляет собой канонический изоморфизм V на V^{**}.

Доказательство. Прежде всего, утверждается, что $u^{**} \in V^{**}$. В самом деле, следующее вычисление показывает аддитивность u^{**}:

$$(\phi + \psi)u^{**} = (\phi + \psi)(u) = \phi(u) + \psi(u) = (\phi)u^{**} + (\psi)u^{**}.$$

Однородность u^{**} доказывается аналогично:

$$(\lambda\phi)u^{**} = (\lambda\phi)(u) = \lambda\phi(u) = \lambda(\phi)u^{**}.$$

Далее, утверждается, что отображение $u \mapsto u^{**}$ линейно. В самом деле, в силу линейности ϕ имеем

$$(\phi)(u+v)^{**} = \phi(u+v) = \phi(u) + \phi(v) = (\phi)u^{**} + (\phi)v^{**}$$

и для любого $\lambda \in R$,

$$(\phi)(u\lambda)^{**} = \phi(u\lambda) = \phi(u)\lambda = (\phi)u^{**}\lambda.$$

Таким образом, действительно

$$(u+v)^{**} = u^{**} + v^{**}, \qquad (u\lambda)^{**} = u^{**}\lambda.$$

Наконец, утверждается, что ядро отображения $u \mapsto u^{**}$ равно 0. В самом деле, равенство $u^{**} = 0$ означает, что $\phi(u) = (\phi)u^{**} = 0$ для всех $\phi \in V^*$, что невозможно, если $u \neq 0$. В самом деле, любой вектор $u \neq 0$ можно выбрать в качестве первого вектора базиса и тогда, конечно, $u^*(u) = 1$ для соответствующей координатной функции u^*.

Пусть теперь $e_1, \dots, e_n$ — базис в V, $e_1^*, \dots, e_n^*$ — двойственный базис V^* и $e_1^{**}, \dots, e_n^{**}$ — двойственный базис в V^{**}. По определению

$$(e_i^*)e_j^{**} = \delta_{ij} = e_i^*(e_j).$$

Если размерность $\dim(V)$ бесконечна, то даже над полем V^{**} не может быть изоморфно V. Дело в том, что в этом случае $\dim(V^*) > \dim(V)$. Гомоморфизм $V \longrightarrow V^{**}$, $v \mapsto v^{**}$, продолжает оставаться инъективным, но никогда не является сюръективным. Поэтому в функциональном анализе в качестве двойственного к V пространства рассматривается не пространство V^* *всех* линейных функционалов, а гораздо меньшее пространство V' линейных функционалов *непрерывных* по отношению к некоторой топологии V. Пространство V называется **рефлективным**, если $V'' \longrightarrow V$, $v \mapsto v^{**}$, является изоморфизмом топологических векторных пространств. В соответствии с только что доказанным конечномерные векторные пространства рефлективны.

§ 4♢. Двойственное линейное отображение

Пусть $\phi : U \longrightarrow V$ — линейное отображение правых R-модулей. Сейчас мы построим линейное отображение $\phi^* : V^* \longrightarrow U^*$ левых R-модулей. А именно, для любого $\theta \in V^*$ и любого $u \in U$ положим

$$((\theta)\phi^*)(u) = \theta(\phi(u)) = (\theta \circ \phi)(u).$$

Так как это равенство верно для любого $u \in U$, мы можем положить

$$(\theta)\phi^* = \theta \circ \phi.$$

Иными словами, отображение ϕ^* сопоставляет линейному функционалу на V его композицию с ϕ, которая, очевидно, является линейным функционалом на U. Сейчас мы покажем, что это *единственный* способ определить двойственное линейное отображение так, чтобы оно было согласовано с каноническим спариванием.

Теорема. *Для любого линейного отображения $\phi : U \longrightarrow V$ существует единственное линейное отображение $\phi^* : V^* \longrightarrow U^*$ такое, что*

$$\langle (\theta)\phi^*, u\rangle = \langle \theta, \phi(u)\rangle.$$

Доказательство. Единственность ϕ^* очевидна, если ψ^* — другое отображение такое, что $\langle (\theta)\psi^*, u\rangle = \langle \theta, \phi(u)\rangle$ для всех $\theta \in V^*$ и $u \in U$, то, в силу невырожденности спаривания между U и U^* имеем $(\theta)\phi^* = (\theta)\psi^*$, для всех $\theta \in V^*$, но это и значит, что $\phi^* = \psi^*$.

Для доказательства существования зафиксируем $\theta \in V^*$ и рассмотрим отображение $u \mapsto \langle \theta, \phi(u)\rangle$ как функцию на U. В силу линейности спаривания по второму аргументу она линейна и, значит, принадлежит U^*. Обозначим ее через $(\theta)\phi^*$. Осталось заметить, что в силу линейности спаривания по первому аргументу сопоставление $\theta \mapsto (\theta)\phi^*$ линейно.

Теорема. *Пусть x — матрица ϕ в базисах $e_1, \dots, e_n$, $f_1, \dots, f_m$. Тогда матрица двойственного линейного отображения ϕ^* в двойственных базисах $f_1^*, \dots, f_m^*$ и $e_1^*, \dots, e_n^*$ равна x.*

Доказательство. Отождествим вектор $u \in U$ со столбцом координат в базисе $e_1, \dots, e_n$, а столбец $\phi(u) \in V$ со столбцом коордиан в базисе $f_1, \dots, f_m$. По определению матрицы линейного отображения для *правых* модулей имеем $\phi(u) = xu$.

Проделаем теперь такую же операцию с элементами *левых* модулей V^* и U^* в двойственных базисах. При этом элементы двойственных модулей истолковываются как строки, а спаривания $U^* \times U \longrightarrow R$ и $V^* \times V \longrightarrow R$ — как умножение строки на столбец. Таким образом, утверждение теоремы представляет собой просто еще одну форму ассоциативности умножения, $\theta(xu) = (\theta x)(u)$.

Теорема. *Двойственное линейное отображение обладает следующими свойствами:*

- $(\phi + \psi)^* = \phi^* + \psi^*$;
- $(\lambda\phi)^* = \phi^*\lambda$;
- $(\phi\psi)^* = \psi^*\phi^*$;
- $\mathrm{id}_V^* = \mathrm{id}_{V^*}$;
- $\phi^{**} = \phi$.

Доказательство. Все эти свойства вытекают непосредственно из определения. Для модулей конечного ранга еще проще воспользоваться проведенным в предыдущей теореме вычислением матрицы двойственного линейного отображения.

§ 5♢. Двойственность для подмодулей

Определим **левый ортогонал** к подмодулю $U \leq V$ как

$$^{\perp}U = \{\phi \in V^* \mid \phi(u) = 0 \text{ для всех } u \in U\}.$$

Правый ортогонал к подмодулю $M \leq V^*$ определяется совершенно аналогично:
$$M^\perp = \{v \in V \mid \phi(v) = 0 \text{ для всех } \phi \in M\}.$$
Совершенно очевидно, что ${}^\perp U$ подмодуль в V^*, а $M^\perp$ подмодуль в V. Из этих определений непосредственно очевидно, что переход к ортогоналу обращает включения.

Лемма. *Для любых подмодулей $U, W \leq V$ и $M, N \leq V^*$ имеем*
$$U \leq W \quad \Longleftrightarrow \quad {}^\perp U \geq {}^\perp W, \qquad\qquad M \leq N \quad \Longleftrightarrow \quad M^\perp \geq N^\perp.$$

Теорема. *Предположим, что V конечномерно и $U \leq V$. Тогда*
$$U^* \cong V^*/{}^\perp U.$$

Доказательство. Рассмотрим ограничение
$$\mathrm{res}_U^V : V^* \longrightarrow U^*, \qquad \phi \mapsto \phi|_U.$$
Тогда ${}^\perp U$ есть в точности ядро этого отображения.

Таким образом, для векторных пространств получаем.

Следствие 1. *Имеет место равенство*
$$\dim(V) = \dim(U) + \dim({}^\perp U).$$

Для *конечномерных* векторных пространств отсюда вытекает такое замечательное следствие.

Следствие 2. *Пусть* $\dim(V) < \infty$. *Тогда для любого подмодуля $U \leq V$ имеет место равенство $({}^\perp U)^\perp = U$.*

Доказательство. В самом деле, ясно, что $({}^\perp U)^\perp \geq U$. С другой стороны, предыдущее следствие и его аналог с заменой правых модулей на левые, показывают, что
$$\dim(U) + \dim({}^\perp U) = \dim(V) = \dim(V^*) = \dim({}^\perp U) + \dim({}^\perp U)^\perp.$$
Таким образом, $\dim({}^\perp U)^\perp = \dim(U)$. Но это и значит, что $({}^\perp U)^\perp = U$.

Разумеется, для бесконечномерных пространств и для свободных модулей конечного ранга над кольцом это, вообще говоря, совершенно неверно. В этих случаях, как правило, $({}^\perp U)^\perp$ строго больше, чем U. Для равенства U должно, по крайней мере, выделяться прямым слагаемым, а для модулей над кольцом это бывает крайне редко.

Следующий результат выражает двойственность между суммой и пересечением подмодулей.

Теорема. *Пусть* $\dim(V) < \infty$. *Тогда для любых двух подпространств* $U, W \leq V$ *имеют место равенства*

$$^{\perp}(U \cap W) = {}^{\perp}U + {}^{\perp}W, \qquad {}^{\perp}(U + W) = {}^{\perp}U \cap {}^{\perp}W.$$

Доказательство. Из леммы 1 вытекает, что ${}^{\perp}U, {}^{\perp}W \leq {}^{\perp}(U \cap W)$, а ${}^{\perp}(U + W) \leq {}^{\perp}U, {}^{\perp}W$ и, значит,

$${}^{\perp}U + {}^{\perp}W \leq {}^{\perp}(U \cap W), \qquad {}^{\perp}(U + W) \leq {}^{\perp}U \cap {}^{\perp}W.$$

Таким образом, нам осталось лишь доказать совпадение соответствующих размерностей. Это утверждение представляет собой в точности теорему о размерности суммы и пересечения. В самом деле,

$$\begin{aligned}\dim({}^{\perp}U + {}^{\perp}W) = \dim({}^{\perp}U) + \dim({}^{\perp}W) - \dim({}^{\perp}U \cap {}^{\perp}W)) \geq \\ \dim({}^{\perp}U) + \dim({}^{\perp}W) - \dim({}^{\perp}(U + W)) = \\ \dim(V) - \dim(U) - \dim(W) + \dim(U + W) = \\ \dim(V) - \dim(U \cap W) = \dim({}^{\perp}(U \cap W)),\end{aligned}$$

как и утверждалось.

Проверка совпадения размерностей для второго случая совершенно аналогична и читатель может провести ее самостоятельно. Впрочем, делать это не нужно, так как совпадение размерностей во втором случае эквивалентно их совпадению в первом случае. В этом можно убедиться, например, так:

$$\begin{aligned}\dim({}^{\perp}(U \cap W))) + \dim({}^{\perp}(U + W)) = \\ 2\dim(V) - \dim(U \cap W) - \dim(U + W) = 2\dim(V) - \dim(U) - \dim(W) = \\ \dim({}^{\perp}U) + \dim({}^{\perp}W) = \dim({}^{\perp}U + {}^{\perp}W) + \dim({}^{\perp}U \cap {}^{\perp}W).\end{aligned}$$

Мы только что убедились, что первые слагаемые в левой и правой частях совпадают. Но тогда, конечно, совпадают и вторые слагаемые.

Следствие. *Если* $V = U \oplus W$, *то* $V^* = {}^{\perp}U \oplus {}^{\perp}W$.

§ 6◊. Теорема Фредгольма

> Don't answer me rashly, — because many, I know, quote the book who have not read it, — and many have read it who understand it not: — If either of these is your case, as I write to instruct, I will tell you in three words what the book is.
>
> Laurence Sterne. Tristram Shandy, Vol. II, Ch. II

В настоящем параграфе мы вскроем подлинный механизм альтернативы Фредгольма. С точки зрения рассмотренной в настоящей главе теории она состоит в двойственности между ядрами и образами.

В параграфе 4 мы сопоставили каждому линейному отображению $\phi : U \longrightarrow V$ двойственное линейное отображение

$$\phi^* : V^* \longrightarrow U^*, \qquad \theta \mapsto \theta \circ \phi.$$

При таком определении следующее утверждение практически очевидно — по крайней мере для векторных пространств. Между тем, это одна из замечательных классических теорем математики, из которой вытекают чрезвычайно важные следствия.

Теорема Фредгольма. *Имеют место следующие равенства*

$$\operatorname{Ker}(\phi^*) = {}^\perp \operatorname{Im}(\phi), \qquad \operatorname{Im}(\phi^*) = {}^\perp \operatorname{Ker}(\phi).$$

Доказательство. Первое равенство совершенно очевидно. В самом деле, $\operatorname{Im}(\phi) = \{\phi(u), u \in U\}$, и поэтому

$${}^\perp \operatorname{Im}(\phi) = \{\theta \in V^* \mid \forall u \in U, \mid \theta(\phi(u)) = 0\} = \{\theta \in V^* \mid \theta \circ \phi = 0\} = \operatorname{Ker}(\phi^*).$$

Для конечномерных векторных пространств второе равенство сразу следует отсюда при помощи второй дуализации (замените ϕ на ϕ^* и примените следствие 2 предыдущего параграфа). Однако, для общего случая нужно независимое доказательство и сейчас мы увидим, что оно несколько сложнее, чем доказательство первой части. Это не должно нас удивлять, так как даже в теории множеств существование одностороннего обратного для инъективного отображения (т.е. то, что мы только что проделали) очевидно, а вот существование одностороннего обратного для сюръективного отображения гарантируется только аксиомой выбора. Тем более, она должна использоваться в нашем случае. Проще всего использовать аксиому выбора в форме Хана—Банаха: любой линейный функционал на подпространстве продолжается до линейного функционала на всем пространстве.

В самом деле, $\operatorname{Ker}(\phi) = \{u \in U \mid \phi(u) = 0\}$, и поэтому

$${}^\perp \operatorname{Ker}(\phi) = \{\theta \in U^* \mid \phi(u) = 0 \Longrightarrow \theta(u) = 0\} = \{\theta \in U^* \mid \operatorname{Ker}(\theta) \geq \operatorname{Ker}(\phi)\}.$$

По теореме о гомоморфизме каждый такой гомоморфизм θ пропускается через $\operatorname{Im}(\phi) = U/\operatorname{Ker}(\phi)$. Иными словами, существует такой линейный функционал $\eta \in \operatorname{Im}(\phi)^*$, что $\theta = \eta \circ \phi$. Так как $\operatorname{Im}(\phi)$ выделяется прямым слагаемым, то η можно продолжить на все V, например, положив его равным 0 на каком-то дополнении к $\operatorname{Im}(\phi)$. Так как нас интересуют только значения η на элементах $\operatorname{Im}(\phi)$, мы продолжаем обозначать получившийся линейный функционал на V той же буквой η. Таким образом, правая часть равна

$$\{\eta \circ \phi \mid \eta \in V^*\} = \operatorname{Im}(\phi^*),$$

как и утверждалось.

Сформулируем несколько непосредственных следствий теоремы Фредгольма.

Следствие 1. *Имеют место следующие эквивалентности.*

- ϕ *эпиморфизм* $\Longleftrightarrow$ ϕ^* *мономорфизм.*
- ϕ *мономорфизм* $\Longleftrightarrow$ ϕ^* *эпиморфизм.*
- ϕ *изоморфизм* $\Longleftrightarrow$ ϕ^* *изоморфизм.*

Следующая переформулировка этого утверждения называется **альтернативой Фредгольма**.

Следствие 2. *Система* $ax = v$ *имеет решение при любой правой части в том и только том случае, когда система* $ya = 0$ *имеет только тривиальное решение.*

Доказательство. $\mathrm{Ker}(\phi^*)^{\perp} = \mathrm{Im}(\phi)$.

Следствие 3. *Пусть* $\phi : U \longrightarrow V$ *— фредгольмов оператор. Тогда двойственный оператор* $\phi^* : V^* \longrightarrow U^*$ *тоже фредгольмов и*

$$\mathrm{ind}(\phi^*) = -\,\mathrm{ind}(\phi).$$