Алгебра, первый курс, четвертый модуль

Е. Ю. Смирнов

Аннотация. Записки лекций по алгебре для первого курса факультета математики ВШЭ, весна 2012/13 учебного года

1. Первая лекция, 4 апреля 2013 г.

В предыдущей части курса рассматривались вопросы, связанные с делимости, разложением на множители и т.д. в кольцах целых чисел и многочленов. Наша ближайшая задача — обобщить эти понятия на более широкий класс колец. Для начала напомним определение кольца́.

1.1. Кольца, поля, идеалы.

Определение 1.1. *Кольцо* (точнее, коммутативное ассоциативное кольцо с единицей — пока что мы будем рассматривать только такие) — это множество A, снабжённое двумя бинарными операциями, сложением и умножением, удовлетворяющими следующим аксиомам:

(A1-A4): A является абелевой группой по сложению;
(M1): умножение коммутативно: $ab = ba$ для любых $a, b \in A$;
(M2): умножение ассоциативно: $a(bc) = (ab)c$ для любых $a, b, c \in A$;
(M3): существование единицы: $\exists 1 \in A$: $\forall a \in A\ 1 \cdot a = a$;
(D): дистрибутивность: $(a + b)c = ac + bc$

Замечание 1.2. Мы не требуем того, что $1 \neq 0$. Однако если единица равна нулю, то кольцо A состоит только из нуля (докажите это!)

Замечание 1.3. Если $1 \neq 0$ и выполнена аксиома существования обратного по умножению:

(M4): $\forall a \in A\ \exists a^{-1} \in A$: $a \cdot a^{-1} = 1$,

---

Вы используете эти записки на свой страх и риск. Никто не гарантирует, что их текст полностью соответствует содержанию лекций. Тем более не гарантируется отсутствие в этом тексте ошибок. Впрочем, о найденных ошибках лучше сообщать автору.

то такое кольцо называется *полем*.

В дальнейшем буквой $\mathbb{K}$ (от немецкого Körper) мы без дополнительных оговорок будем называть произвольное поле.

Определение 1.4. Пусть A — произвольное кольцо. Подмножество $I \subset A$ называется *идеалом*, если выполнено следующее:

I1: $\forall x, y \in I\ x + y \in I$;
I2: $\forall x \in I\ -x \in I$;
I3: $\forall x \in I$, $a \in A$ верно, что $ax \in I$.

Первые две аксиомы равносильны тому, что I — подгруппа в A по сложению (в частности, $0 \in I$). Обратите внимание, что в третьей аксиоме требуется замкнутость I по умножению на *все* элементы из A (а не только из I) — это очень существенное ограничение.

В частности, если $I \ni 1$, то $I = A$: единицу можно умножить на любой элемент кольца, и результат будет снова принадлежать I. По той же причине идеал, содержащий любой *обратимый* элемент, совпадает со всем кольцом.

Приведем несколько примеров идеалов.

Пример 1.5. В любом кольце есть два тривиальных идеала: нулевой (состоящий из одного нуля) и всё кольцо. Впрочем, некоторые авторы предпочитают считать, что $I \neq A$, и всё кольцо, таким образом, идеалом не считается — но это вопрос терминологический.

Пример 1.6. Пусть $d \in \mathbb{Z}$. Множество $(d) = \{dm \mid m \in \mathbb{Z}\} \subset \mathbb{Z}$ является идеалом в $\mathbb{Z}$. Чуть позже мы проверим, что всякий идеал в $\mathbb{Z}$ имеет такой вид.

Пример 1.7. Пусть $a_1, \ldots, a_m \in A$ — некоторое подмножество элементов кольца. *Идеал, порожденный* $a_1, \ldots, a_m$, обозначается $(a_1, \ldots, a_m)$. Это минимальный по включению идеал, содержащий эти элементы. Ясно, что он имеет вид

$$(a_1, \ldots, a_m) = \{a_1x_1 + \cdots + a_mx_m \mid x_1 \ldots, x_m \in A\}.$$

В предыдущем примере можно было взять любое подмножество в A, не обязательно конечное, и породить им идеал.

Вот ещё один пример, который оказывается очень важным в алгебраической геометрии.

Пример 1.8. Пусть $A = \mathbb{K}[x_1, \ldots, x_n]$, $S \subset \mathbb{K}^n$ — произвольное подмножество точек в n-мерном аффинном пространстве. Множество функций, равных нулю во всех точках S, образует идеал в A.

1.2. Кольца главных идеалов.

Определение 1.9. Идеал вида $(a) \subset A$, т.е. порождённый одним элементом, называется *главным идеалом*.

Определение 1.10. Целостное кольцо A называется *кольцом главных идеалов*, если все идеалы в нём являются главными.

Предложение 1.11. *$\mathbb{Z}$ и $\mathbb{K}[x]$ — кольца главных идеалов.*

Доказательство. Пусть I — ненулевой идеал в $\mathbb{Z}$. Выберем в нём наименьший положительный элемент и обозначим его через d. Докажем, что $I = (d)$. Действительно, пусть $x \in I$. Разделим x на d с остатком: $x = dq + r$. Значит, $r = x - dq$. Оба слагаемых в правой части принадлежат I, значит, $r \in I$. Но $0 \leq r < d$. Поэтому $r = 0$, и x делится на d нацело. Значит, $x \in (d)$.

Случай $\mathbb{K}[x]$ разбирается аналогично, только в качестве d надо взять элемент наименьшей степени. □

Упражнение 1.12. Докажите, что $\mathbb{Z}[x]$ и $\mathbb{K}[x, y]$ не являются кольцами главных идеалов.

1.3. Евклидовы кольца. Неформально говоря, евклидовыми называются кольца, в которых возможно деление с остатком (т.е. алгоритм Евклида).

Определение 1.13. Целостное кольцо A называется *евклидовым*, если в нём существует функция *нормы*, или *высоты*,

$$n\colon A \setminus \{0\} \to \mathbb{Z}_{\geq 0},$$

удовлетворяющая аксиомам:

E1: $n(xy) \geq n(x)$ для любых $x, y \in A$;
E2: Для любых $x, y \in A$, где $y \neq 0$, найдутся такие $q, r \in A$, что $x = qy + r$, причём либо $n(y) > n(r)$, либо $r = 0$.

Упражнение 1.14. Докажите, что аксиома (E1) на самом деле является избыточной: а именно, если на A существует функция, удовлетворяющая (E2), то из неё можно изготовить функцию (вообще говоря, другую), удовлетворяющую обеим аксиомам.

Примеры 1.15. Кольца $\mathbb{Z}$, $\mathbb{K}[x]$, $\mathbb{K}[[x]]$ являются евклидовыми. Нормами в них являются соответственно модуль целого числа, степень многочлена и порядок нуля степенного ряда (т.е. номер первого ненулевого коэффициента).

Предложение 1.16. *Всякое евклидово кольцо является кольцом главных идеалов.*

Доказательство. Это доказывается аналогично предложению 1.11, при помощи выбора в идеале элемента наименьшей нормы. □

Замечание 1.17. Бывают (достаточно экзотические) примеры колец главных идеалов, не являющихся евклидовыми. Таким, например, является кольцо $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$. Задача со звёздочкой: докажите это.

1.4. Делимость в кольцах главных идеалов. В этом разделе A — кольцо главных идеалов.

Дадим определение наибольшего общего делителя двух элементов. Привычное определение придётся модифицировать, т.к. в произвольном кольце не совсем понятно, что такое “наибольший”.

Определение 1.18. Пусть $a, b \in A$. *Наибольшим общим делителем* элементов a, b (обозначение: (a, b)) называется такой элемент d, что $d \mid a$ и $d \mid b$, и при этом d делится на *любой другой* общий делитель элементов a и b.

При таком определении a priori неясно, что НОД двух элементов вообще существует. Однако это несложно доказать.

Предложение 1.19. *В кольце главных идеалов у любых двух элементов $a, b \in A$ существует наибольший общий делитель, который выражается через них в виде $d = ax + by$.*

Доказательство. Рассмотрим идеал $(a, b) \subset A$. Он главный; пусть он порождён элементом d. Это значит, что $d = ax + by$. Докажем, что d — НОД элементов a и b. Действительно, поскольку $a, b \in (a, b) = (d)$, оба этих элемента делятся на d. Пусть e — какой-то другой общий делитель a и b. Поскольку $e \mid a$ и $e \mid b$, получаем, что $e \mid ax + by = d$, что и требовалось. □

Определение 1.20. Если $(a, b) = 1$, то a и b называются *взаимно простыми*.

1.5. Существование и единственность разложения на простые. Введем понятие *ассоциированных* элементов. Два элемента a и b называются ассоциированными (обозначение: $a\tilde{b}$), если $a = bs$, где s обратим. Иными словами, элементы a и b ассоциированы, если идеалы (a) и (b) совпадают.

Простое число — это такое число, которое делится на единицу и на себя. Обобщим это понятие на произвольные кольца.

Определение 1.21. Необратимый ненулевой элемент p кольца A называется *простым*, если его нельзя представить в виде $p = ab$, где a и b — необратимые элементы. Иными словами, всякий делитель простого элемента p ассоциирован либо с 1, либо с p.

Замечание 1.22. Простые элементы в кольце многочленов обычно называют *неприводимыми*.

Наша ближайшая цель — доказать существование и единственность разложения элемента в произведение простых в кольцах главных идеалов. Сначала докажем следующую лемму.

Лемма 1.23. *Пусть A — кольцо главных идеалов, элемент p прост, и $p \mid a_1 \dots a_n$. Тогда $p \mid a_i$ при некотором i.*

Доказательство. Сначала докажем лемму при $n = 2$. Пусть $p \mid ab$. Допустим, что $p \not| a$; покажем, что $p \mid b$. Действительно, если p не делит a, то p и a взаимно просты. Напишем линейное выражение их НОДа:

$$1 = px + ay.$$

Домножим обе части равенства на b:

$$b = pbx + aby.$$

Правая часть делится на p, так как ab делится на p. Значит, b делится на p.

Случай произвольного n доказывается индукцией по числу сомножителей. □

Отсюда следует единственность разложения элемента кольца главных идеалов на простые множители (с точностью до ассоциированности) — аналог основной теоремы арифметики. Доказательство в этом случае также почти не отличается от случая кольца целых чисел.

Теорема 1.24. *Пусть A — кольцо главных идеалов, $a \in A$ — необратимый элемент, причём*

$$a = p_1 \dots p_n = q_1 \dots q_m,$$

где p_i, q_i простые. Тогда $n = m$, причём $q_1, \dots, q_n$ можно перенумеровать так, что каждый из q_i станет ассоциированным с соответствующим p_i.

Доказательство. Пусть $n \leq m$. Докажем теорему индукцией по n. База: при $n = 1$ доказывать нечего.

Переход. Поскольку $p_1 \mid q_1 \dots q_m$, в силу предыдущей леммы p_1 делит некоторый q_i. Без ограничения общности будем считать, что $i = 1$. Поскольку q_1 также прост, получаем, что $p_1 \tilde{q}_1$. Стало быть, обе части равенства $p_1 \dots p_n = q_1 \dots q_m$ можно сократить на p_1 и получить равенство $p_2 \dots p_n = s q_2 \dots q_m$, где s обратим. Мы свели теорему к случаю $n - 1$ сомножителя, а для него она верна по предположению индукции. □

Теперь докажем *существование* разложения элемента в произведение простых. Это утверждение, которое в $\mathbb{Z}$ очевидно, в случае произвольного кольца главных идеалов приходится доказывать. Кроме того, бывают кольца (не являющиеся кольцами главных идеалов), в которых разложения элемента в произведение простых не существует.

Теорема 1.25. *В кольце главных идеалов каждый ненулевой необратимый элемент может быть разложен на простые множители.*

Доказательство. Пусть это не так, и существуют элементы, которые не раскладываются в произведение простых. Назовём их *плохими*. Пусть a_0 — плохой элемент. Тогда он раскладывается в произведение двух необратимых элементов (иначе он был бы простым), причём хотя бы один из сомножителей обязан также быть плохим. Пусть $a_0 = a_1 b_1$, и a_1 плохой. То же самое верно про a_1: он раскладывается в произведение $a_2 b_2$, где a_2 плохой, и так далее до бесконечности. Мы получили бесконечный ряд элементов

$$a_0, a_1, \ldots, a_n, \ldots,$$

где $a_i \mid a_{i-1}$. Поэтому имеет место бесконечная строго возрастающая цепочка идеалов

$$(a_0) \subset (a_1) \subset \cdots \subset (a_n) \subset \ldots.$$

Докажем, что в кольце главных идеалов такой цепочки быть не может. Рассмотрим объединение всех идеалов цепочки: $I = \bigcup_{i=0}^{\infty}(a_i)$. Это тоже идеал (почему?). Пусть $I = (d)$ (ведь A — кольцо главных идеалов!). Тогда элемент d лежит в каком-то из (a_n) для некоторого n. Стало быть, $(a_n) = (a_{n+1}) = I$ — противоречие с тем, что цепочка строго возрастает. Стало быть, всякий элемент разлагается на простые множители. □

Замечание 1.26. Это же рассуждение проходит для существенно более широкого класса колец: так называемых *нётеровых колец*, в которых каждый идеал конечно порождён. Поэтому в нётеровых кольцах имеет место существование разложения в произведение простых — а вот единственности там может и не быть.

Определение 1.27. Целостное кольцо, в котором каждый ненулевой необратимый элемент разлагается в произведение простых, причём единственным (в смысле теоремы 1.25) образом, называется *факториальным*.

Это определение позволяет объединить теоремы 1.25 и 1.24:

Теорема 1.28. *Всякое кольцо главных идеалов факториально.*

2. Вторая лекция, 4 апреля 2013 г.

2.1. Факторкольца. Ранее мы рассматривали конструкцию факторгруппы по нормальной подгруппе. Для колец есть её непосредственный аналог: факторкольцо по идеалу.

Пусть A — произвольное коммутативное кольцо, $I \subset A$ — идеал. Определим на множестве элементов из A следующее отношение: будем говорить, что $x \equiv y \mod I$, если $x-y \in I$. Ясно, что это отношение эквивалентности. Классы эквивалентности — это множества вида $x + I = \{x + a \mid a \in I\}$. Иногда мы также будем обозначать класс $x+I$ через $[x]$. Обозначим множество этих классов через A/I.

На классах эквивалентности из A/I можно определить операции сложения и умножения:

$$(x + I) + (y + I) = (x + y) + I; \qquad (x + I)(y + I) = xy + I.$$

Предложение 2.1. *Заданные таким образом операции определены корректно, т.е. сумма и произведение классов не зависят от выбора их представителей.*

Доказательство. Проверим корректность умножения: пусть $x \equiv x' \mod I$ и $y \equiv y' \mod I$. Тогда $x' = x' + a$, $y' = y + b$, где $a, b \in I$. Поэтому

$$x'y' = (x + a)(y + b) = xy + ay + xb + ab \equiv xy \mod I,$$

поскольку ay, xb и ab лежат в I. Корректность сложения проверяется аналогично. □

Таким образом, на A/I вводятся операции сложения и умножения, что задаёт на нём структуру кольца. Полученное кольцо называется *факторкольцом* кольца A по идеалу I.

Ясно, что нулём и единицей в A/I являются $0 + I$ и $1 + I$ соответственно.

Упражнение 2.2. Докажите утверждение, обратное к предыдущему предложению: пусть $I \subset A$ — абелева подгруппа по сложению, причем операция умножения, заданная на классах эквивалентности из A/I, определена корректно. Покажите, что I — идеал в A.

2.2. Гомоморфизмы.

Определение 2.3. Пусть A, B — два произвольных кольца. Отображение $f\colon A \to B$ называется *гомоморфизмом*, если оно сохраняет операции: а именно,

$$f(x + y) = f(x) + f(y), \qquad f(xy) = f(x)f(y).$$

Пусть A, B — два произвольных кольца. Отображение $f\colon A \to B$ называется *гомоморфизмом*, если оно сохраняет операции: а именно,

$$f(x + y) = f(x) + f(y), \qquad f(xy) = f(x)f(y).$$

Замечание 2.4. В определении мы *не требуем*, чтобы единица переходила в единицу. Так, например, вложение $A \to A \oplus A$, $a \mapsto (a, 0)$ — гомоморфизм, хотя единицу в единицу он не переводит.

Упражнение 2.5. Докажите, что $\operatorname{Im} f \subset B$ — подкольцо в B, а $\operatorname{Ker} f \subset A$ — идеал в A.

Говорят, что гомоморфизм инъективен/сюръективен/биективен, если он инъективен/сюръективен/биективен как отображение множеств. Такие гомоморфизмы ещё называют соответственно *мономорфизмами*, *эпиморфизмами* и *изоморфизмами*.

Пример 2.6. Важный пример гомоморфизма — отображение факторизации $\pi\colon A \to A/I$, $\pi(a) = a + I$, где I — произвольный идеал в кольце A. Ясно, что π — эпиморфизм.

Следующая теорема утверждает, что всякий эпиморфизм является отображением факторизации по некоторому идеалу. Аналоги этой теоремы для факторгрупп и факторпространств уже разбирались ранее.

Теорема 2.7 (о гомоморфизме колец). *Пусть* $f\colon A \to B$ — *гомоморфизм колец. Тогда* $\operatorname{Im} f \simeq A/\operatorname{Ker} f$. *Более точно, отображение* $\varphi\colon \operatorname{Im} f \to A/\operatorname{Ker} f$, *при котором* $b = f(a) \in \operatorname{Im} f$ *отображается в* $\pi(a) = a + \operatorname{Ker} f$, *есть изоморфизм.*

Доказательство. Из теоремы о гомоморфизме групп следует, что отображение φ является изоморфизмом абелевых групп. Осталось проверить, что оно сохраняет умножение. Действительно, пусть $f(x) = u$, $f(y) = v$. Тогда $f(xy) = uv$, и

$$\varphi(uv) = \pi(xy) = \pi(x)\pi(y) = \varphi(u)\varphi(v),$$

что и требовалось. □

Пример 2.8. Рассмотрим отображение

$$\varphi\colon \mathbb{K}[x] \to \mathbb{K}, \qquad f(x) \mapsto f(a)$$

вычисления значения многочлена в точке a. Ясно, что это гомоморфизм, причём сюръективный (значение многочлена в данной точке может быть любым). При этом по теореме Безу ядро φ есть

$$\operatorname{Ker} \varphi = \{f \in \mathbb{K}[x] \mid f(a) = 0\} = (x - a).$$

Значит, $\mathbb{K}[x]/(x - a) \cong \mathbb{K}$.

Пример 2.9. Рассмотрим теперь отображение вычисления значения *вещественного* многочлена в точке i:

$$\mathbb{R}[x] \to \mathbb{C}, \qquad f(x) \mapsto f(i).$$

Это гомоморфизм, причем также сюръективный (проверьте это!). Кроме того, если $f(i) = 0$, то $f(-i) = f(\bar{i}) = \overline{f(i)} = 0$, поэтому $f(x) \vdots (x-i)(x+i) = x^2 + 1$. Значит,

$$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}.$$

Упражнение 2.10. Чему изоморфно факторкольцо $\mathbb{R}[x]/(x^2 + px + q)$? (ответ зависит от знака дискриминанта квадратного трёхчлена).

2.3. Китайская теорема об остатках. Сначала напомним понятие прямой суммы колец.

Определение 2.11. *Прямая сумма* $A \oplus B$ колец A и B — это кольцо, элеменами которого являются пары (a, b), где $a \in A$, $b \in B$, а сложение и умножение задаются покомпонентно.

Заметим, что подкольца $\{(a, 0)\} \cong A$ и $\{(0, b)\} \cong B$ являются идеалами в $A \oplus B$.

Вернёмся к кольцам главных идеалов. В них также имеет место аналог китайской теоремы об остатках, который очень просто формулируется и доказывается с помощью понятия факторкольца.

Теорема 2.12 (Китайская теорема об остатках). *Пусть A — кольцо главных идеалов, элементы $u, v \in A$ взаимно просты. Тогда*

$$A/(uv) \simeq A/(u) \oplus A/(v).$$

Доказательство. Поскольку u и v взаимно просты, через них можно линейно выразить единицу:

$$1 = au + bv.$$

Рассмотрим гомоморфизм

$$f\colon A \to A/(u) \oplus A/(v), \qquad f(x) = (x + (u), x + (v)).$$

Тогда $f(bv) = f(1 - au) = (1, 0)$, $f(au) = f(1 - bv) = (0, 1)$. Следовательно, гомоморфизм f сюръективен. Очевидно, что его ядро — это идеал (uv). Поэтому требуемое утверждение следует из теоремы о гомоморфизме колец. □

2.4. Максимальные и простые идеалы.

Определение 2.13. Идеал $\mathfrak{m} \subset A$ называется максимальным, если он не содержится ни в каком большем идеале (не совпадающем со всем кольцом).

Определение 2.14. Идеал $\mathfrak{p} \subset A$ называется простым, если для любых двух элементов $a, b \in A$, таких, что $ab \in \mathfrak{p}$, верно, что либо $a \in \mathfrak{p}$, либо $b \in \mathfrak{p}$.

Пример 2.15. Простые идеалы в $\mathbb{Z}$ — это идеалы вида (p), где p простое. Они же являются и максимальными (проверьте это!).

Предложение 2.16. *1) Идеал $\mathfrak{p}$ прост тогда и только тогда, когда $A/\mathfrak{p}$ — область целостности.*
2) Идеал $\mathfrak{m}$ максимален тогда и только тогда, когда $A/\mathfrak{m}$ — поле.

Доказательство. 1) Пусть $\mathfrak{p}$ прост, $ab \in \mathfrak{p}$. Значит, a или b лежат в $\mathfrak{p}$. Рассмотрим их образы при отображении факторизации $A \to A/\mathfrak{p}$. Получим, что из $[ab] = [0]$ следует, что $[a] = [0]$ или $[b] = [0]$, что и означает, что $A/\mathfrak{p}$ целостное. Обратное утверждение доказывается точно так же.

2) Пусть $\mathfrak{m}$ максимален. Докажем, что всякий ненулевой элемент $[a] \in A/\mathfrak{m}$ обратим. Действительно, $a \notin \mathfrak{m}$. Рассмотрим идеал $a + \mathfrak{m} = \{ax + m \mid x \in A, m \in \mathfrak{m}\}$. Этот идеал содержит $\mathfrak{m}$ и не совпадает с ним (поскольку содержит ещё и a), значит, он совпадает со всем кольцом. Поэтому $1 = ax + m$ для некоторых $x \in A$,$m \in \mathfrak{m}$. Получаем, что в $A/\mathfrak{m}$ элемент $[x]$ есть $[a]^{-1}$, так как $[1] = [a][x] + [m] = [a][x]$. Обратное утверждение доказывается аналогично (проделайте это!). □

Следствие 2.17. *Всякий максимальный идеал прост.*

Упражнение 2.18. Приведите пример простого, но не максимального идеала.

Оказывается, что в кольцах главных идеалов верно и обратное к следствию 2.17. Это вытекает из следующей теоремы.

Теорема 2.19. *Пусть A — кольцо главных идеалов, $u \in A$ — необратимый элемент. Тогда $A/(u)$ является полем тогда и только тогда, когда u прост.*

Доказательство. Пусть u не прост: $u = vw$, где v и w необратимы. Тогда в $A/(u)$ получаем: $[v][w] = [u] = [0]$, причём $[v] \neq [0]$ и $[w] \neq [0]$ — значит, $A/(u)$ не область целостности, и тем более не поле.

Обратно, пусть u прост. Это значит, что для любого $x \notin (u)$ верно, что $(x, u) = 1$, следовательно, найдутся a и b, для которых $ax + bu = 1$. Значит, в $A/(u)$ получаем, что $[a][x] = [1]$, т.е. $[a]$ обратим. □

3. Третья лекция, 11 апреля 2013 г.

3.1. Модули над кольцами: определение. Как известно, векторное пространство — это множество V, снабжённое двумя операциями: сложением (относительно которого оно является абелевой группой) и умножением на элементы фиксированного поля $\mathbb{K}$. Что будет, если попробовать заменить в этом определении поле $\mathbb{K}$ на произвольное кольцо?

Например, всякая абелева группа является "векторным пространством над $\mathbb{Z}$": действительно: её элементы можно складывать между собой, а также умножать на целые числа по правилу $n \cdot g = g + \cdots + g$ (всего n слагаемых, с очевидными изменениями, если $n < 0$). Это мотивирует следующее

Определение 3.1. Пусть A — коммутативное ассоциативное кольцо с единицей. *Модуль* над кольцом A (или A-*модуль*) — это абелева группа, снабжённая действием кольца A, т.е. операцией $A \times M \to M$, удовлетворяющей следующим условиям:

(M1): $(ab)m = a(bm)$ для любых $a, b \in A$, $m \in M$;
(M2): $1 \cdot m = m$ для любого $m \in M$;
(D1): $(a + b)m = am + bm$ для любых $a, b \in A$, $m \in M$;
(D2): $a(m + n) = am + an$ для любых $a \in A$, $m, n \in M$.

Пример 3.2. Если $A = \mathbb{K}$ — поле, то M есть не что иное, как векторное пространство над $\mathbb{K}$.

Пример 3.3. Если $A = \mathbb{Z}$, то M — это просто абелева группа.

Пример 3.4 (очень важный!). Пусть $A = \mathbb{K}[x]$, V — векторное пространство над $\mathbb{K}$, $\mathcal{A} \in \mathrm{End}(V)$ — линейный оператор на V. Тогда V является $\mathbb{K}[x]$-модулем, на котором действие кольца многочленов задано так:

$$(a_n x^n + \cdots + a_1 x + a_0) \cdot v = a_n \mathcal{A}^n v + \cdots + a_1 \mathcal{A} v + a_0 v.$$

Иными словами, x действует на V при помощи оператора $\mathcal{A}$. Отметим, что разные линейные операторы задают *разные* структуры модуля на V.

Пример 3.5. Всякое кольцо A является модулем над самим собой. Аксиомы (M1), (M2), (D1) и (D2) при этом следуют из определения кольца́.

3.2. Подмодули, фактормодули, гомоморфизмы.

Определение 3.6. Пусть M — модуль над A. $N \subset M$ называется *подмодулем* в M, если $n + n' \in N$ и $an \in N$ для любых $a \in A$ и $n, n' \in N$.

Пример 3.7. Подмодули модулей из примеров 3.2 и 3.3 — это векторное подпространство и абелева подгруппа соответственно.

Пример 3.8. Подмодуль модуля из примера 3.4 — это *$\mathcal{A}$-инвариантное* подпространство $U \subset V$ (т.е. такое подпространство, для которого $\mathcal{A}u \in U$ для любого $u \in U$).

Пример 3.9. Подмодуль модуля из примера 3.5 — это идеал $I \subset A$.

По подмодулям можно брать факторы.

Определение 3.10. Пусть $N \in M$ — подмодуль. Рассмотрим отношение эквивалентности на M: $m \equiv m' \mod N$, если $m - m' \in N$. Множество классов эквивалентности $m + N = [m]$ называется *факторомодулем* и обозначается через M/N. Операции на M/N задаются обычным образом:

$$(m + N) + (n + N) = (m + n) + N; \qquad a(m + N) = am + N.$$

Упражнение 3.11. Проведите сами все необходимые проверки корректности.

Пример 3.12. Пусть A — кольцо, $I \subset A$ — идеал. Тогда A/I тоже является A-модулем.

Определение 3.13. Отображение A-модулей $f\colon M \to N$ называется *гомоморфизмом*, если

$$f(x + y) = f(x) + f(y); \qquad f(ax) = af(x)$$

для любых $x, y \in M$, $a \in A$.

Упражнение 3.14. Проверьте, что $\operatorname{Ker} f$ и $\operatorname{Im} f$ — подмодули в M и N соответственно.

Пример 3.15. Пусть $N \subset M$ — модуль и подмодуль. Отображение

$$\pi\colon M \to M/N, \qquad m \mapsto m + N$$

является сюръективным гомоморфизмом (=эпиморфизмом). Оно называется *эпиморфизмом факторизации.*

Соответственно, имеется и теорема о гомоморфизме:

Теорема 3.16 (о гомоморфизме модулей). *Пусть $f\colon M \to N$ — гомоморфизм A-модулей. Тогда $\operatorname{Im} f \simeq M/\operatorname{Ker} f$. Более точно, отображение $\varphi\colon \operatorname{Im} f \to M/\operatorname{Ker} f$, при котором $b = f(a) \in \operatorname{Im} f$ отображается в $\pi(a) = a + \operatorname{Ker} f$, есть изоморфизм.*

Доказательство. Докажите эту теорему сами. □

3.3. Системы порождающих. Конечно порождённые и циклические модули. Пусть M — A-модуль, $S \subset M$ — произвольное подмножество. Рассмотрим *наименьший* подмодуль в M, содержащий S. Это

$$\langle S \rangle = \{a_1 x_1 + \cdots + a_s x_s \mid x_i \in S, a_i \in A\}.$$

Если $\langle S \rangle = M$, то S называют *системой порождающих* модуля M. Если M допускает конечную систему порождающих, то он называется *конечно порождённым*.

Пример 3.17. $\mathbb{Q}$ как $\mathbb{Z}$-модуль не является конечно порождённым.

Пример 3.18. Конечно порождённые $\mathbb{K}$-модули — это в точности конечномерные векторные пространства.

Определение 3.19. Модуль, порождённый одним элементом, называется *циклическим*.

Пример 3.20. Всякий циклический $\mathbb{Z}$-модуль изоморфен либо $\mathbb{Z}$, либо $\mathbb{Z}/m\mathbb{Z}$.

Пусть M — произвольный A-модуль. Рассмотрим множество

$$\operatorname{Ann} M = \{a \in A \mid am = 0 \quad \forall m \in M\} \subset A.$$

Оно называется *аннулятором* модуля M. Ясно, что $\operatorname{Ann} M$ — идеал в A.

Нетрудно видеть, что имеется биекция между циклическими A-модулями и идеалами в A:

Теорема 3.21. *Всякий циклический A-модуль M изоморфен A/I, где I — идеал в A, причем $I = \operatorname{Ann} M$.*

Доказательство. Ясно, что если I — идеал в A, то A/I — циклический модуль. Докажем обратное: пусть $M = \langle x \rangle$ — циклический модуль. Рассмотрим гомоморфизм A-модулей

$$f\colon A \to M, \qquad a \mapsto ax.$$

Ясно, что f сюръективен, и $\operatorname{Ker} f = \operatorname{Ann} M$. Но по теореме о гомоморфизме $M \cong A/\operatorname{Ker} f$. □

3.4. Базис. Свободные модули. Как и в случае векторных пространств, для модулей имеют смысл понятия линейной зависимости и базиса.

Определение 3.22. Элементы $x_1, \ldots, x_n \in M$ называются *линейно независимыми*, если для любых $a_1, \ldots, a_n \in A$, не равных нулю одновременно, $a_1 x_1 + \cdots + a_n x_n \neq 0$. Линейно независимая система порождающих A-модуля M называется его *базисом*.

В отличие от векторных пространств, не у всякого модуля имеется базис. Так, например, в $\mathbb{Z}/(m)$ базиса нет — поскольку даже всякая система из *одного* элемента оказывается линейно зависимой (поскольку $mx = 0$ для любого $x \in \mathbb{Z}/(m)$).

Определение 3.23. Конечно порождённый модуль, обладающий базисом, называется *свободным*.

Скажем, всякий свободный циклический модуль изоморфен A.

Далее мы будем считать, что A — кольцо главных идеалов.

Теорема 3.24. *Все базисы свободного A-модуля L содержат одинаковое число элементов.*

Доказательство. Если $A = \mathbb{K}$ — поле, то это просто теорема о размерности векторного пространства.

Пусть теперь A — не поле. Выберем в нём произвольный простой элемент $p \in A$. Мы знаем, что $A/(p)$ — поле.

Рассмотрим в модуле L подмодуль pL, полученный как образ гомоморфизма $\mu_p\colon x \mapsto px$. В фактормодуле L/pL идеал $(p) \subset A$ действует нулём, поэтому L/pL является векторным пространством над $A/(p)$ (продумайте этот момент!).

Если $e_1, \ldots, e_n$ — базис в L, то классы базисных элементов $[e_1], \ldots, [e_n]$ будут образовывать базис в L/pL как в модуле над $A/(p)$ — то есть как в векторном пространстве. А, как известно, все базисы векторного пространства состоят из одинакового числа элементов. □

Определение 3.25. Число элементов в базисе свободного модуля называется его *рангом*.

В силу предыдущей теоремы это определение корректно.

Всякий свободный модуль L изоморфен $A^{\oplus r}$, где r — ранг L. Изоморфизм, как и в случае векторных пространств, определяется выбором базиса в L.

4. Четвертая лекция, 11 апреля 2013 г.

Я, возможно, напишу записки этой лекции когда-нибудь потом. А пока почитайте лучше какую-нибудь книжку. Например, эту: Э. Б. Винберг, *Курс алгебры*, гл. 9, §3. Там все написано.

И вообще читайте побольше книжек. Желательно и художественных тоже, а не только про математику.

5. Пятая лекция, 16 мая 2013 г.

5.1. Полилинейные отображения.

Определение 5.1. Пусть $V_1, \dots, V_k, W$ — векторные пространства (над некоторым полем K, которое мы фиксируем по крайней мере до конца этой лекции). Отображение

$$\varphi\colon V_1 \times \dots \times V_k \to W$$

называется *полилинейным*, если оно линейно по каждому из аргументов:

$$\varphi(\dots, \lambda v_i + \mu v_i', \dots) = \lambda\varphi(\dots, v_i, \dots) + \mu\varphi(\dots, v_i', \dots).$$

Пример 5.2. 1-линейные отображения — это обычные линейные отображения $\varphi\colon V_1 \to W$. Если $W = K$, то 1-линейные отображения — это линейные функционалы на V_1, а 2-линейные отображения — это билинейные формы.

Полилинейные отображения можно складывать и умножать на элементы поля K. Поэтому они образуют векторное пространство. Будем обозначать его через $\operatorname{Hom}(V_1, \dots, V_k; W)$. Несложно найти его размерность:

Предложение 5.3. *Пусть* $\dim V_i = d_i$, $\dim W = d$. *Тогда*

$$\dim \operatorname{Hom}(V_1, \dots, V_k; W) = d_1 \dots d_k \cdot d.$$

Доказательство. Фиксируем базисы в наших векторных пространствах: пусть $e_1^{(i)}, \dots, e_{d_i}^{(i)}$ — базис в V_i, $e_1, \dots, e_d$ — базис в W. В силу полилинейности отображение φ однозначно определяется своими значениями на всевозможных наборах базисных векторов $\varphi(e_{\alpha_1}^{(1)}, \dots, e_{\alpha_k}^{(k)})$; если $v_i = \sum x_{\alpha_i}^{(i)} e_{\alpha_i}^{(i)}$, то

$$\varphi(v_1, \dots, v_k) = \sum_{1 \le \alpha_i \le d_i} x_{\alpha_1}^{(1)} \dots x_{\alpha_k}^{(k)} \varphi(e_{\alpha_1}^{(1)}, \dots, e_{\alpha_k}^{(k)}).$$

Разложив каждый из векторов $\varphi(e_{\alpha_1}^{(1)}, \dots, e_{\alpha_k}^{(k)})$ по базису $e_1, \dots, e_d$ пространства W, получим $(k+1)$-мерную матрицу размера $d_1 \times \dots \times d_k \times d$, однозначно определяющую отображение φ.

Предъявим базис пространства $\operatorname{Hom}(V_1, \dots, V_k; W)$. Его образуют, например, следующие отображения:

$$\delta^j_{(i_1,\dots,i_k)}\colon (e_{\alpha_1}^{(1)}, \dots, e_{\alpha_k}^{(k)}) \mapsto \begin{cases} e_j, & \text{если } (i_1, \dots, i_k) = (\alpha_1, \dots, \alpha_k); \\ 0 & \text{иначе.} \end{cases}$$

Здесь $1 \le j \le d$, $1 \le i_r \le d_r$. □

5.2. Тензорное произведение. Пусть V, W — векторные пространства с базисами $\{e_i \mid i \in I\}$ и $\{f_j \mid j \in J\}$ соответственно (вообще говоря, не предполагается, что множества I и J конечны).

Предложение 5.4. *Следующие свойства билинейного отображения $\varphi V \times W \to U$ эквивалентны:*

(1) *$\varphi(e_i, f_j)$ составляют базис в W;*
(2) *для любого $u \in U$ существует единственное представление $u = \sum_{i \in I} \varphi(e_i, w_i)$, где $w_i \in W$;*
(3) *для любого $u \in U$ существует единственное представление $u = \sum_{j \in J} \varphi(v_j, f_j)$, где $v_j \in V$.*

Доказательство. Докажем, что (1) эквивалентно (2). Действительно, если $u = \sum_{i \in I, j \in J} x_{ij} \varphi(e_i, f_j)$, то $u = \sum_{i \in I} \varphi(e_i, w_i)$, где $w_i = \sum_{j \in J} x_{ij} f_j$ (здесь мы пользуемся линейностью φ по второму аргументу). Аналогично доказывается, что (1) эквивалентно (3). □

Следствие 5.5. *Выполнение условия (1) не зависит от выбора базисов в V и W.*

Доказательство. Действительно, условие (1) эквивалентно условию (3), которое никак не использует выбор базиса в V. По тем же причинам (1) не зависит от выбора базиса в W. □

Определение 5.6. *Тензорное произведение* пространств V и W — это векторное пространство T вместе с билинейным отображением

$$\otimes \colon V \times W \to T,$$

удовлетворяющим условию: если $\{e_i \mid i \in I\}$ и $\{f_j \mid j \in J\}$ — базисы в V и W соответственно, то $\{e_i \times f_j\}$ — базис в T.

В силу предыдущего следствия выполнение последнего условия не зависит от выбора базисов в V и W.

Очевидно, что для любых V и W такие билинейное отображение и пространство T существуют: достаточно взять в качестве T пространство, порождённое базисными элементами t_{ij}, где $i \in I$, $j \in J$, и определить отображение по правилу $e_i \otimes f_j \mapsto t_{ij}$. Кроме того, легко убедиться в его единственности:

Предложение 5.7. *Пространство T и отображение $\otimes$ заданы однозначно в следующем смысле: если $(T_1, \otimes_1)$ и $(T_2, \otimes_2)$ — два тензорных произведения пространств V и W, то существует единственный изоморфизм*

$$\psi \colon T_1 \to T_2, \qquad \psi(v \otimes_1 w) = v \otimes_2 w \qquad \forall v \in V, w \in W.$$

Доказательство. Искомый изоморфизм задаётся на базисных элементах по правилу $\psi(e_i \otimes_1 f_j) = e_i \otimes_2 f_j$. □

Итак, пространство T и отображение $\otimes$ определены однозначно по V и W. Будем обозначать T через $V \otimes W$. Из явного описания базиса в $V \otimes W$ немедленно следует такое

Предложение 5.8. *Если V и W конечномерны, то* $\dim V \otimes W = \dim V \cdot \dim W$.

Следующий пример показывает, как обстоит дело в случае счётномерных пространств.

Пример 5.9. Пусть $V = K[x]$, $W = K[y]$. Тогда $K[x] \otimes K[y] \cong K[x, y]$.

Действительно, изоморфизм строится по правилу: $f(x) \otimes g(y) \mapsto f(x)g(y)$. $K[x, y]$ действительно будет тензорным произведением $K[x]$ и $K[y]$, т.к. множество образов пар базисных векторов (x^m, y^n) образует базис $\{x^m y^n\}$ в $K[x, y]$.

5.3. Универсальное свойство. Оказывается, что $V \otimes W$ является в каком-то смысле "самым главным" из пространств, которые могут быть образами билинейных отображений из $V \times W$.

Предложение 5.10 (универсальное свойство тензорного произведения). *Для любого билинейного отображения $\varphi\colon V \times W \to U$ существует единственное* линейное *отображение $F\colon V \otimes W \to U$, для которого $\varphi(v, w) = F(v \otimes w)$.*

Доказательство. Искомое отображение задаётся на базисных элементах пространства $V \otimes W$:

$$F(e_i \otimes f_j) := \varphi(e_i, f_j).$$

□

Замечание 5.11. Можно (и в каком-то смысле даже более правильно) принять универсальное свойство за определение $V \otimes W$ и после этого доказать существование пространства и отображения, определяемого универсальным свойством.

Упражнение 5.12. Выведите из универсального свойства предложение 5.7 (т.е. утверждение о том, что тензорное произведение определено однозначно с точностью до изоморфизма).

5.4. Ещё примеры тензорных произведений. Далее V и W будут конечномерными векторными пространствами, с базисами $\{e_1, \dots, e_m\}$ и $\{f_1, \dots, f_n\}$ соответственно. Пусть $\{\xi_1, \dots, \xi_m\}$ и $\{\eta_1, \dots, \eta_n\}$ — двойственные базисы в V^* и W^* соответственно.

Рассмотрим произведение $V^* \times W$. Определим отображение из него в пространство $\mathrm{Hom}(V; W)$, т.е. в пространство линейных отображений из V в W, по следующему правилу. Паре $\alpha \in V^*$, $w \in W$ будет сопоставляться отображение $\alpha \otimes w$, для которого

$$(\alpha \otimes w)(v) = \alpha(v) \cdot w.$$

Легко видеть, что $\operatorname{Ker}(\alpha \otimes w) = \operatorname{Ker}\alpha$, а $\operatorname{Im}(\alpha \otimes w) = \langle w \rangle$. Поэтому все отображения вида $\alpha \otimes w$ имеют ранг 1. Легко видеть, что верно и обратное: всякое отображение из V в W ранга 1 имеет вид $\alpha \otimes w$.

Мы получили билинейное отображение $V^* \times W \to \operatorname{Hom}(V; W)$. По универсальному свойству, оно соответствует некоторому линейному отображению $V^* \otimes W \to \operatorname{Hom}(V, W)$. Посмотрим на то, куда оно переводит базисные векторы, т.е. $\xi_i \otimes f_j$. Отображение, соответствующее паре базисных векторов $\xi_i \otimes f_j$, записывается матричной единицей E_{ji}. Эти матрицы образуют базис пространства $\operatorname{Hom}(V, W)$, значит, полученное отображение есть изоморфизм. Мы доказали

Предложение 5.13. $V^* \otimes W \cong \operatorname{Hom}(V; W)$.

Замечание 5.14. Обратите внимание, что в образе билинейного отображения $V^* \times W \to \operatorname{Hom}(V; W)$ содержатся *не все* линейные отображения, а только имеющие ранг 1. Однако каждое линейное отображение может быть представлено в виде линейной комбинации отображений ранга 1. Более подробно мы обсудим это в следующей лекции.

Упражнение 5.15. Рассуждая аналогично, покажите, что

$$V^* \otimes W^* \cong \operatorname{Hom}(V, W; K)$$

(правая часть есть пространство билинейных форм на $V \times W$).

5.5. Тензорное произведение операторов. Пусть даны два пространства V и W, на каждом из которых задано по линейному оператору $\mathcal{A} \in \operatorname{End}(V)$ и $\mathcal{B} \in \operatorname{End}(W)$. Определим тогда линейный оператор $\mathcal{A} \otimes \mathcal{B}$ на пространстве $V \otimes W$ по правилу

$$(\mathcal{A} \otimes \mathcal{B})(v \otimes w) = \mathcal{A}v \otimes \mathcal{B}w.$$

Пусть оператор $\mathcal{A}$ в базисе $e_1, \ldots, e_m$ записывается матрицей $A = (a_{ij})$, а оператор $\mathcal{B}$ в базисе $f_1, \ldots, f_n$ записывается матрицей B. Тогда несложно убедиться, что матрица оператора $\mathcal{A} \otimes \mathcal{B}$ в базисе $e_1 \otimes f_1, e_1 \otimes f_2, \ldots, e_1 \otimes f_n, e_2 \otimes f_1, \ldots, e_m \otimes f_n$ записывается в блочном виде:

$$\begin{pmatrix} a_{11}B & a_{12}B & \ldots & a_{1m}B \\ a_{21}B & a_{22}B & \ldots & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \ldots & a_{mm}B \end{pmatrix}$$

Из этой записи следует, что $\operatorname{tr}(\mathcal{A} \otimes \mathcal{B}) = \operatorname{tr}\mathcal{A} \cdot \operatorname{tr}\mathcal{B}$.

Упражнение 5.16. Выразите $\det(\mathcal{A} \otimes \mathcal{B})$ через $\det\mathcal{A}$ и $\det\mathcal{B}$.

6. Шестая лекция, 21 мая 2013 г.

6.1. Расширения полей. Это важный пример, показывающий, как тензорное произведение встречается "в реальной жизни". Пусть $L \supset K$ — поле, содержащее основное поле K в качестве подполя (например, $L = \mathbb{C}$, $K = \mathbb{R}$). В частности, L является векторным пространством над K. Пусть V — какое-то еще векторное пространство над K. Рассмотрим тензорное произведение

$$V(L) = L \otimes_K V.$$

Это векторное пространство над K, но его несложно превратить в векторное пространство над L; для этого определим в $V(L)$ умножение на элементы из L так:

$$\lambda(\mu \otimes v) = \lambda\mu \otimes v.$$

Можно считать, что V вкладывается в $V(L)$ как векторное пространство над K: при вложении $v \mapsto 1 \otimes v$. Если $e_1, \dots, e_n$ — базис V как векторного пространства над K, то векторы $1 \otimes e_1, \dots, 1 \otimes e_n$ будут образовывать базис $V(L)$ *как векторного пространства над* L. В частности, $\dim_K V = \dim_L V(L)$. Таким образом, про $V(L)$ можно думать как про V, в котором мы разрешили умножать на скаляры из L, а не только из K.

Обратно, $V(L)$ можно рассматривать как векторное пространство над K размерности $\dim_K V \cdot \dim_K L$, базис в котором образован элементами вида $\theta_i \otimes e_j$. Здесь $\theta_1, \dots, \theta_d$ — базис L как векторного пространства над K.

Например, в случае $L = \mathbb{C}$, $K = \mathbb{R}$ мы получаем утверждение о том, что всякий вектор из $V(\mathbb{C})$ представи́м в виде $v + iw$, где $v, w \in V$. В этом случае пространство $V(\mathbb{C})$ называется *комплексификацией* пространства V.

6.2. Свойства тензорного произведения.

Предложение 6.1. *Имеют место следующие канонические (т.е. не зависящие от выбора базисов) изоморфизмы:*

(1) $V \otimes W \cong W \otimes V$;
(2) $V \otimes (W \otimes U) \cong (V \otimes W) \otimes U$;
(3) $V \otimes (W \oplus U) \cong V \otimes W \oplus V \otimes U$.

Упражнение 6.2. Докажите это предложение.

Из этого предложения, в частности, следует, что можно говорить о $V_1 \otimes \dots \otimes V_k$, не заботясь о порядке расстановки скобок.

Упражнение 6.3. Дайте определение тензорного произведения нескольких пространств, аналогичное 5.6, и докажите, что полученное пространство изоморфно $(\dots (V_1 \otimes V_2) \otimes \dots \otimes V_k)$.

Для тензорного произведения k пространств верны (с очевидными модификациями) все те факты, которые мы доказывали в прошлой лекции для тензорного произведения двух пространств. Так, имеется изоморфизм

$$\operatorname{Hom}(V_1 \otimes \dots \otimes V_k; W) \cong \operatorname{Hom}(V_1, \dots, V_k; W),$$

определяемый по правилу

$$F(v_1 \otimes v_k) := \varphi(v_1, \dots, v_k).$$

Определение 6.4. Элементы вида $v_1 \otimes \dots \otimes v_k \in V_1 \otimes \dots \otimes V_k$ называются *разложимыми*.

Замечание 6.5. Сумма разложимых элементов, вообще говоря, НЕ БУДЕТ разложимым элементом. Множество разложимых элементов НЕ образует векторное подпространство в $V_1 \otimes \dots \otimes V_k$, хотя и порождает его линейно.

6.3. Отображение Сегре. Рассмотрим k-линейное отображение

$$V_1 \times \dots \times V_k \to V_1 \otimes \dots \otimes V_k, \qquad (v_1, \dots, v_k) \mapsto v_1 \otimes \dots \otimes v_k.$$

Если умножить каждый из v_i на некоторый скаляр λ_i, то соответствующий элемент тензорного произведения умножится на $\lambda_1 \cdot \dots \cdot \lambda_k$, т.е. будет пропорционален $v_1 \otimes \dots \otimes v_k$. Поэтому имеет место отображение произведения *проективизаций* пространств V_i в проективизацию тензорного произведения:

$$\mathbb{P}V_1 \times \dots \times \mathbb{P}V_k \to \mathbb{P}(V_1 \otimes \dots \otimes V_k).$$

Это отображение называется *вложением Сегре*.

Упражнение 6.6. Докажите, что это действительно вложение.

Рассмотрим более подробно случай двух пространств; для удобства введем обозначения $V_1 = U^*$, а $V_2 = V$. Тогда $U^* \otimes V \cong \operatorname{Hom}(U, V)$ (именно для этого отождествления нам и понадобилось сопряжение). Пусть $\dim U^* = m + 1$, $\dim V = n + 1$, а на проективизациях этих пространств имеются однородные координаты $(\xi_0 : \dots : \xi_m)$ и $(y_0 : \dots : y_n)$ соответственно. Тогда имеется отображение

$$\sigma\colon \mathbb{P}^m \times \mathbb{P}^n \cong \mathbb{P}U^* \otimes \mathbb{P}V \to \mathbb{P}(\operatorname{Hom}(U; V)) \cong \mathbb{P}^{mn+m+n},$$

заданное правилом

$$\sigma\colon (\alpha, v) \mapsto \alpha \otimes v.$$

Нетрудно записать это отображение в координатах:

$$\sigma\colon ((\xi_0 : \dots : \xi_m), (y_0 : \dots : y_n)) \mapsto (\dots : \xi_i y_j : \dots).$$

Здесь мы считаем, что в $\mathbb{P}^{mn+m+n}$ введены однородные координаты z_{ij}, занумерованные парами индексов (i, j), где $0 \le i \le m$, а $0 \le j \le n$.

Образ отображения σ можно задать и системой уравнений. Мы получили, что $\operatorname{Im}\sigma \subset \mathbb{P}(\operatorname{Hom}(U;V))$ будет состоять изо всех линейных отображений ранга 1. Отображение имеет ранг 1 тогда и только тогда, когда в соответствующей ему матрице все миноры 2×2 равны нулю. Получаем, что $\operatorname{Im}\sigma$ задается однородными квадратичными уравнениями

$$z_{ij}z_{kl} - z_{il}z_{kj} = 0, \qquad 0 \le i,k \le m, \quad 0 \le j,l \le n.$$

Особенно приятно обстоит дело в случае $m = n = 2$: в этом случае мы получаем отображение

$$\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3,$$

образ которого задается единственным уравнением $z_{00}z_{11} = z_{01}z_{10}$, то есть является квадрикой в $\mathbb{P}^3$. Слои над точками в каждом из $\mathbb{P}^1$, то есть множества $\{\alpha\}\times\mathbb{P}^1$ и $\mathbb{P}^1\times\{v\}$, при этом отображении переходят в два семейства прямолинейных образующих на квадрике.

Упражнение 6.7. Покажите, что $\operatorname{Im}\sigma$ не содержится ни в какой гиперплоскости. (Указание: этот факт уже неоднократно обсуждался в этой лекции).

7. Седьмая лекция, 23 мая 2013

7.1. Тензорная алгебра. Пусть V — векторное пространство. Рассмотрим его тензорные степени $V^{\otimes k} = V \otimes \cdots \otimes V$ (всего k сомножителей). Положим $V^{\otimes 0} = K$ и $V^{\otimes 1} = V$. У нас имеются билинейные отображения $V^{\otimes k} \times V^{\otimes l} \to V^{\otimes (k+l)}$, заданные по правилу $(\omega_1, \omega_2) \mapsto \omega_1 \otimes \omega_2$.

Рассмотрим прямую сумму всех тензорных степеней

$$TV = \bigoplus_{k=0}^{\infty} V^{\otimes k}.$$

Описанные выше билинейные отображения задают на этом пространстве умножение. Иными словами, TV является ассоциативной (но некоммутативной) градуированной алгеброй. V вкладывается в TV как компонента степени 1. Обозначим это вложение через ι.

Если выбрать в V базис $e_1, \ldots, e_n$, то мономы вида $e_{i_1} \otimes \cdots \otimes e_{i_k}$ будут базисом в $V^{\otimes k}$. Таким образом, все такие мономы (для всевозможных k) будут образовывать базис в TV как в векторном пространстве. Отметим, что переменные в этих мономах не коммутируют: $e_1 \otimes e_2 \neq e_2 \otimes e_1$.

Алгебра TV также может быть описана при помощи универсального свойства.

Предложение 7.1. *Пусть A — произвольная ассоциативная K-алгебра. Тогда для любого K-линейного отображения $f\colon V \to A$ имеется единственный гомоморфизм K-алгебр $\alpha\colon TV \to A$, для которого $\alpha \circ \iota = f$.*

Упражнение 7.2. Докажите это.

7.2. Симметрическая степень пространства.

Определение 7.3. Пусть V, U — векторные пространства над K. k-линейное отображение $\varphi\colon V \times \cdots \times V \to U$ называется *симметрическим*, если для любой перестановки $\sigma \in S_k$

$$\varphi(v_{\sigma(1)}, \ldots, v_{\sigma(k)}) = \varphi(v_1, \ldots, v_k).$$

Определение 7.4. Векторное пространство S вместе с симметрическим k-линейным отображением

$$V \times \cdots \times V \to S, \qquad (v_1, \ldots, v_k) \mapsto v_1 \cdot \cdots \cdot v_k$$

называется *k-той симметрической степенью пространства V*, если для некоторого базиса $e_1, \ldots, e_n$ пространства V элементы вида $e_{i_1} \cdot \cdots \cdot e_{i_k}$, где $1 \leq i_1 \leq \cdots \leq i_k \leq n$, составляют базис пространства S.

Предложение 7.5. *Пространство S существует и не зависит от выбора базиса.*

Доказательство. Доказательство существования — явная конструкция. Рассмотрим векторное пространство S с базисом $f_{i_1,\dots,i_k}$, занумерованным неубывающими наборами индексов. Определим отображение на наборах базисных векторов так:

$$V \times \dots \times V \to S, \qquad (e_{i_1}, \dots, e_{i_k}) \mapsto f_{i_1,\dots,i_k}.$$

Независимость от выбора базиса проверяется так. Пусть $e'_1, \dots, e'_n$ — другой базис пространства V. Тогда векторы $e'_{j_1} \cdot \dots \cdot e'_{j_k}$, где $j_1 \le \dots \le j_k$, составляют другой базис пространства S, элементы которого линейно выражаются через элементы первого базиса, и наоборот. □

Упражнение 7.6. Сформулируйте и докажите утверждение о единственности S в духе предложения 5.7

Пространство S обозначается через S^kV. Из определения следует, что $\dim S^kV$ равна количеству неубывающих наборов k чисел от 1 до n, т.е. числу способов разложить k шариков по n ящикам, которое, в свою очередь, равняется $\binom{n+k-1}{k}$.

Симметрические степени тоже можно охарактеризовать при помощи универсального свойства.

Предложение 7.7. *Для любого* симметрического k*-линейного отображения* $\varphi\colon V \times \dots \times V \to U$ *существует единственное* линейное *отображение* $F\colon S^kV \to U$*, для которого* $\varphi(v_1, \dots, v_k) = F(v_1 \cdot \dots \cdot v_k)$.

Доказательство. Определим отображение F на базисных векторах по правилу $F(e_{i_1} \cdot \dots \cdot e_{i_k}) = \varphi(e_{i_1}, \dots, e_{i_k})$, где $i_1 \le \dots \le i_k$. В силу симметричности φ это отображение будет задано корректно (подумайте, что это значит). Далее F продолжается на все S^kV по линейности. □

Как и в случае тензорного произведения, элементы из S^kV вида $v_1 \cdot \dots \cdot v_k$ называются *разложимыми*. Они линейно порождают все пространство S^kV, поэтому чтобы задать линейное отображение из S^kV куда-то еще, его достаточно задать на разложимых элементах (что мы обычно и будем делать).

7.3. Симметрическая степень линейного оператора. Пусть $\mathcal{A}$ — линейный оператор на пространстве V. Зададим линейный оператор $S^k\mathcal{A}$ на пространстве S^kV по правилу

$$(S^k\mathcal{A})(v_1 \cdot \dots \cdot v_k) = (\mathcal{A}v_1) \cdot \dots \cdot (\mathcal{A}v_k).$$

Упражнение 7.8. Проверьте, что $\operatorname{tr} S^2\mathcal{A} = \frac{1}{2}((\operatorname{tr}\mathcal{A})^2 + \operatorname{tr}\mathcal{A}^2)$, и придумайте формулу для $\operatorname{tr} S^3\mathcal{A}$.

7.4. Симметрическая алгебра. По аналогии с отображениями тензорных степеней определим билинейные отображения

$$S^kV \times S^lV \to S^{k+l}V, \qquad (v_1 \dots v_k, v_{k+1} \dots v_{k+l}) \mapsto v_1 \dots v_{k+l}.$$

Рассмотрим прямую сумму всех симметрических степеней (как и в случае тензорных степеней, считаем, что $S^0V = K$, $S^1V = V$):

$$SV = \bigoplus_{k \geq 0} S^kV.$$

Она также является градуированной ассоциативной алгеброй, но, в отличие от тензорной алгебре, она уже будет коммутативной. Она называется *симметрической алгеброй* пространства V.

Предложение 7.9. *Пусть* $\dim V = n$. *Тогда симметрическая алгебра изоморфна алгебре многочленов от* n *переменных:* $SV \cong K[u_1, \dots, u_n]$.

Доказательство. Зададим изоморфизм на базисных векторах:

$$e_{i_1} \cdot \dots \cdot e_{i_k} \mapsto u_{i_1} \cdot \dots \cdot u_{i_k}.$$

□

Упражнение 7.10. Постройте *канонический* изоморфизм $SV \cong K[V^*]$.

7.5. Симметрические тензоры. Симметризация. В этом разделе мы считаем, что $\operatorname{char} K = 0$.

Рассмотрим k-тую тензорную степень $V^{\otimes k}$ пространства V. На этом пространстве действует группа S_k перестановками сомножителей:

$$\sigma(v_1 \otimes \dots \otimes v_k) = v_{\sigma(1)} \otimes \dots \otimes v_{\sigma(k)}.$$

Тензор $\omega \in V^{\otimes k}$ называется *симметрическим*, если $\sigma(\omega) = \omega$ для любой перестановки $\sigma \in S_k$. Симметрические тензоры образуют подпространство, которое мы обозначим через $\operatorname{Sym}^k V \subset V^{\otimes k}$.

Рассмотрим оператор *симметризации* $\operatorname{Sym}\colon V^{\otimes k} \to V^{\otimes k}$:

$$\operatorname{Sym}(\omega) = \frac{1}{k!} \sum_{\sigma \in S_k} \sigma(\omega).$$

Ясно, что $\operatorname{Im}\operatorname{Sym} \subset \operatorname{Sym}^k V$, а также что оператор Sym оставляет симметрические тензоры неподвижными. Поэтому Sym является *проектором* на подпространство $\operatorname{Sym}^k V$.

Пример 7.11. Пусть $V = \langle e_1, \dots, e_n \rangle$. Тогда $\operatorname{Sym}^2 V = \langle e_i \otimes e_i, e_i \otimes e_j + e_j \otimes e_i \rangle$, а $\operatorname{Ker}\operatorname{Sym} = \langle e_i \otimes e_j - e_j \otimes e_i \rangle$.

Предложение 7.12. *Имеется изоморфизм векторных пространств*

$$\mu\colon S^kV \to \operatorname{Sym}^k V, \qquad \mu(v_1 \cdot \dots \cdot v_k) = \operatorname{Sym}(v_1 \otimes \dots \otimes v_k).$$

Доказательство. Правая часть симметрична и полилинейна относительно $v_1, \dots, v_k$. Значит, в силу универсального свойства существует линейное отображение $\mu\colon S^k V \to \operatorname{Sym}^k V$. Можно проверить (проделайте это), что при этом отображении базисные векторы вида $e_{i_1} \cdot \dots \cdot e_{i_k}$ переходят в $\operatorname{Sym}(e_{i_1} \otimes \dots \otimes e_{i_k})$. Такие векторы составляют базис пространства $\operatorname{Sym}^k V$, значит, μ — изоморфизм. $\square$

Замечание 7.13. Итак, в каждой из тензорных степеней есть подпространство, изоморфное k-той симметрической степени: $\operatorname{Sym}^k V \subset V^{\otimes k}$. Однако прямая сумма $\bigoplus \operatorname{Sym}^k V \subset TV$ всех этих пространств *не является* подалгеброй относительно обычного тензорного произведения, т.к. не замкнута относительно этой операции. Чтобы ввести на $\bigoplus \operatorname{Sym}^k V$ структуру алгебры, следует определить умножение по правилу

$$\omega \cdot \tau = \operatorname{Sym}(\omega \otimes \tau).$$

8. Восьмая лекция, 30 мая 2013 г.

Эта лекция посвящена конструкции внешних степеней и внешней алгебры векторного пространства. Эта конструкция во многом схожа с конструкцией симметрических степеней, поэтому мы приведем часть утверждений без доказательства, рассчитывая на то, что читатель восстановит доказательства сам по аналогии с предыдущей лекцией.

8.1. Внешние степени векторного пространства.

Определение 8.1. Пусть V, U — векторные пространства над K. k-линейное отображение $\varphi\colon V \times \cdots \times V \to U$ называется *кососимметрическим*, если для любой перестановки $\sigma \in S_k$

$$\varphi(v_{\sigma(1)}, \ldots, v_{\sigma(k)}) = (-1)^\sigma \varphi(v_1, \ldots, v_k),$$

где $(-1)^\sigma$ — это знак перестановки σ.

Замечание 8.2. Если среди аргументов кососимметрического отображения присутствуют два одинаковых вектора (или, более общо, набор линейно зависимых векторов), то значение отображения на этом наборе равно нулю (убедитесь в этом!).

Определение 8.3. Векторное пространство Λ вместе с кососимметрическим k-линейным отображением

$$V \times \cdots \times V \to \Lambda, \qquad (v_1, \ldots, v_k) \mapsto v_1 \wedge \cdots \wedge v_k$$

называется *k-той внешней степенью пространства V*, если для некоторого базиса $e_1, \ldots, e_n$ пространства V элементы вида $e_{i_1} \wedge \cdots \wedge e_{i_k}$, где $1 \leq i_1 < \cdots < i_k \leq n$, составляют базис пространства Λ.

Предложение 8.4. *Пространство Λ существует, не зависит от выбора базиса и определено однозначно с точностью до изоморфизма.*

Доказательство. Доказательство этого предложения дословно повторяет доказательство аналогичного утверждения о симметрических степенях. □

Пространство Λ обозначается через $\Lambda^k V$. Из определения следует, что $\dim \Lambda^k V$ равна количеству строго возрастающих наборов k чисел от 1 до n, т.е. числу способов выбрать k предметов из n возможных, т.е. $\binom{n}{k}$.

Обратите внимание, что при $k = n$ пространство $\Lambda^k V$ будет *одномерно*, а при $k > n$ оно и вовсе оказывается равным нулю! В этом существенная разница с симметрическим случаем.

Для внешних степеней тоже имеется универсальное свойство.

Предложение 8.5. *Для любого* кососимметрического k*-линейного отображения* $\varphi\colon V\times\dots\times V\to U$ *существует единственное* линейное *отображение* $F\colon \Lambda^k V\to U$*, для которого* $\varphi(v_1,\dots,v_k)=F(v_1\wedge\dots\wedge v_k)$.

Доказательство аналогично симметрическому случаю.

Элементы из $\Lambda^k V$ (их еще иногда называют *кососимметрическими поливекторами*, или k*-векторами*) вида $v_1\wedge\dots\wedge v_k$ называются *разложимыми*.

Пусть в V выбран базис $e_1,\dots,e_n$. Пространство $\Lambda^k V$ можно воспринимать как пространство однородных форм степени k от переменных $e_1,\dots,e_n$, которые *антикоммутируют*, т.е. удовлетворяют соотношениям $e_i\wedge e_j=-e_j\wedge e_i$ (и, в частности, $e_i\wedge e_i=0$).

8.2. Внешняя степень линейного оператора. Пусть $\mathcal{A}$ — линейный оператор на пространстве V. Зададим линейный оператор $\Lambda^k\mathcal{A}$ на пространстве $\Lambda^k V$ по правилу

$$(\Lambda^k\mathcal{A})(v_1\wedge\dots\wedge v_k)=(\mathcal{A}v_1)\wedge\dots\wedge(\mathcal{A}v_k).$$

Упражнение 8.6. Проверьте, что $\operatorname{tr} S^2\mathcal{A}=\frac{1}{2}((\operatorname{tr}\mathcal{A})^2-\operatorname{tr}\mathcal{A}^2)$, и придумайте формулу для $\operatorname{tr}\Lambda^3\mathcal{A}$.

Дальнейшее отличается от симметрического случая. Пусть $k=n$. Пространство $\Lambda^n V$ одномерно, т.е. оператор $\Lambda^n\mathcal{A}\colon\Lambda^n V\to\Lambda^n V$ есть просто умножение на скаляр. Вычислим этот скаляр. Выберем в V базис $e_1,\dots,e_n$, в котором оператор $\mathcal{A}$ действует матрицей $A=(a_{ij})$. Возьмем в $\Lambda^n V$ единственный базисный вектор $e_1\wedge\dots\wedge e_n$ и посмотрим, как на него действует $\Lambda^n\mathcal{A}$.

$$\begin{aligned}\Lambda^n\mathcal{A}(e_1\wedge\dots\wedge e_n)&=(\mathcal{A}e_1)\wedge\dots\wedge(\mathcal{A}e_n)=\\&=\left(\sum_{i_1=1}^{n}a_{i_1 1}e_{i_1}\right)\wedge\dots\wedge\left(\sum_{i_n=1}^{n}a_{i_n n}e_{i_n}\right)=\\&=\sum_{\{i_1,\dots,i_n\}=\{1,\dots,n\}}a_{i_1 1}a_{i_2 2}\dots a_{i_n n}e_{i_1}\wedge\dots\wedge e_{i_n}=\\&=\sum_{\sigma\in S_n}a_{\sigma(1)1}a_{\sigma(2)2}\dots a_{\sigma(n)n}e_{\sigma(1)}\wedge\dots\wedge e_{\sigma(n)}=\\&=\left(\sum_{\sigma\in S_n}(-1)^\sigma a_{\sigma(1)1}a_{\sigma(2)2}\dots a_{\sigma(n)n}\right)e_1\wedge\dots\wedge e_n=\\&=\det\mathcal{A}\cdot e_1\wedge\dots\wedge e_n.\end{aligned}$$

Мы доказали следующее

Предложение 8.7. *Пусть* $\dim V=n$, $\mathcal{A}\in\operatorname{End}(V)$. *Тогда оператор* $\Lambda^n\mathcal{A}$ *действует на одномерном пространстве* $\Lambda^n V$ *скаляром* $\det\mathcal{A}$.

Упражнение 8.8. Докажите аналогичным образом формулу для разложения определителя по столбцу.

Указание 8.9. Воспользуйтесь тем, что $\Lambda^n\mathcal{A}(e_1\wedge\dots\wedge e_n) = \Lambda^{n-1}\mathcal{A}(e_1\wedge\dots\wedge e_{n-1})\wedge\mathcal{A}e_n$.

Упражнение 8.10. Докажите, что след оператора $\Lambda^k\mathcal{A}$ равен с точностью до знака коэффициенту при λ^{n-k} характеристического многочлена оператора $\mathcal{A}$.

8.3. Грассманова алгебра. Рассмотрим билинейные отображения

$$\wedge\colon \Lambda^kV\times\Lambda^lV\to\Lambda^{k+l}V,\qquad (v_1\wedge\dots\wedge v_k, v_{k+1}\wedge\dots\wedge v_{k+l})\mapsto v_1\wedge\dots\wedge v_{k+l}.$$

Рассмотрим прямую сумму всех внешних степеней (как и ранее, считаем, что $\Lambda^0V = K$, $\Lambda^1V = V$):

$$\Lambda V = \bigoplus_{k\geq 0}\Lambda^kV.$$

Она также является градуированной ассоциативной алгеброй, произведение в которой мы обозначим знаком $\wedge$. Она называется *грассмановой*, или *внешней алгеброй* пространства V.

В отличие от симметрического случая, внешняя алгебра будет конечномерна: ее размерность будет равна $\binom{n}{0}+\binom{n}{1}+\dots+\binom{n}{n} = 2^n$ — что неудивительно, поскольку базис в ней образуют всевозможные векторы вида $e_{i_1}\wedge\dots\wedge e_{i_k}$, где $\{i_1,\dots,i_k\}$ может быть любым подмножеством множества $\{1,\dots,n\}$ (в том числе пустым).

Внешняя алгебра не будет коммутативной, зато будет *суперкоммутативной*: для любых двух однородных элементов ω_1 и ω_2 степеней k и l соответственно, имеет место равенство

$$\omega_1\wedge\omega_2 = (-1)^{kl}\omega_2\wedge\omega_1.$$

(докажите это сами).

8.4. Кососимметрические тензоры. Альтернирование. В этом разделе мы считаем, что $\operatorname{char}K = 0$.

Рассмотрим k-тую тензорную степень $V^{\otimes k}$ пространства V. Напомним, что группа S_k действует на ней перестановками сомножителей:

$$\sigma(v_1\otimes\dots\otimes v_k) = v_{\sigma(1)}\otimes\dots\otimes v_{\sigma(k)}.$$

Тензор $\omega\in V^{\otimes k}$ называется *кососимметрическим*, если $\sigma(\omega) = (-1)^\sigma\omega$ для любой перестановки $\sigma\in S_k$. Кососимметрические тензоры образуют подпространство, которое мы обозначим через $\operatorname{Alt}^kV\subset V^{\otimes k}$.

Рассмотрим оператор *альтернирования* $\operatorname{Alt}\colon V^{\otimes k}\to V^{\otimes k}$:

$$\operatorname{Alt}(\omega) = \frac{1}{k!}\sum_{\sigma\in S_k}(-1)^\sigma\sigma(\omega).$$

Как и в симметрическом случае, Alt будет проектором на подпространство $\mathrm{Alt}^k V$. Это подпространство оказывается изоморфным k-той внешней степени пространства V:

Предложение 8.11. *Имеется изоморфизм векторных пространств*

$$\mu\colon \Lambda^k V \to \mathrm{Alt}^{\,k} V, \qquad \mu(v_1 \wedge \dots \wedge v_k) = \mathrm{Alt}(v_1 \otimes \dots \otimes v_k).$$

Доказательство аналогично симметрическому случаю.

Замечание 8.12. Как и в симметрическом случае, прямая сумма $\bigoplus \mathrm{Alt}^k V \subset TV$ всех пространств кососимметрических тензоров *не является* подалгеброй относительно обычного тензорного произведения, т.к. не замкнута относительно этой операции. Чтобы ввести на $\bigoplus \mathrm{Alt}^k V$ структуру алгебры, следует определить умножение по правилу

$$\omega \wedge \tau = \mathrm{Alt}(\omega \otimes \tau).$$

Упражнение 8.13. Докажите, что $\mathrm{Sym}(\mathrm{Alt}) = \mathrm{Alt}(\mathrm{Sym}) = 0$.

Упражнение 8.14. Докажите, что $V \otimes V = \mathrm{Sym}^2 V \oplus \mathrm{Alt}^2 V$, а при $k > 2$ и при $\dim V > 1$ такого равенства нет: $V^{\otimes k} \neq \mathrm{Sym}^k V \oplus \mathrm{Alt}^k V$.

8.5. Разложимые тензоры и подпространства. Внешние степени оказываются полезными для работы с подпространствами векторного пространства. Имеет место следующий факт.

Теорема 8.15. (1) *Векторы $v_1, \dots, v_k \in V$ линейно зависимы тогда и только тогда, когда $v_1 \wedge \dots \wedge v_k \neq 0$.*

(2) *Пусть $v_1, \dots, v_k$ и $u_1, \dots, u_k$ — два линейно независимых набора векторов. Тогда их линейные оболочки $\langle v_1, \dots, v_k\rangle$ и $\langle u_1, \dots, u_k\rangle$ совпадают тогда и только тогда, когда поливекторы $v_1 \wedge \dots \wedge v_k$ и $u_1 \wedge \dots \wedge u_k$ пропорциональны.*

Доказательство. (1) Докажем, что из линейной зависимости следует обращение поливектора в нуль. Пусть $v_k = \sum_{i=1}^{k-1} \lambda_i v_i$. Тогда $v_1 \wedge \dots \wedge v_k = v_1 \wedge \dots \wedge v_{k-1} \wedge (\sum \lambda_i v_i) = \sum \lambda_i v_1 \wedge \dots \wedge v_{k-1} \wedge v_i = 0$.

Обратно, если $v_1, \dots, v_k$ линейно независимы, их можно дополнить до базиса пространства V. Ему будет соответствовать базис пространства $\Lambda^k V$, и поливектор $v_1 \wedge \dots \wedge v_k$ будет в числе базисных — следовательно, он будет отличен от нуля.

(2) Пускай $\langle v_1, \dots, v_k\rangle = \langle u_1, \dots, u_k\rangle$. Тогда u_i линейно выражаются через v_j, следовательно,

$$u_1 \wedge \dots \wedge u_k = \sum \lambda_{i_1 \dots i_k} v_{i_1} \wedge \dots \wedge v_{i_k}, \qquad 1 \leq i_1, \dots, i_k \leq k$$

Но $v_{i_1} \wedge \dots \wedge v_{i_k}$ равен либо $\pm v_1 \wedge \dots \wedge v_k$, если все индексы $i_1, \dots, i_k$ различны, либо нулю в противном случае. Поэтому $v_1 \wedge \dots \wedge v_k = \lambda u_1 \wedge \dots \wedge u_k$.

Если же $\langle v_1, \dots, v_k\rangle \neq \langle u_1, \dots, u_k\rangle$, то в V можно выбрать такой базис $e_1, \dots, e_n$, что $\langle e_1, \dots, e_k\rangle = \langle v_1, \dots, v_k\rangle$ и $\langle e_{d+1}, \dots, e_{d+k}\rangle = \langle u_1, \dots, u_k\rangle$ при некотором $d > 0$. Векторы $e_1 \wedge \dots \wedge e_k$ и $e_{d+1} \wedge \dots \wedge e_{d+k}$ будут двумя различными (а значит, не пропорциональными друг другу) базисными векторами из $\Lambda^k V$. □

8.6. Грассманиан. Вложение Плюккера.

Определение 8.16. *Грассманианом*, или *многообразием Грассмана* $\mathrm{Gr}(k, V)$ называется множество всех k-мерных подпространств в пространстве V.

Упражнение 8.17 (по курсу топологии). Введите на $\mathrm{Gr}(k, V)$ структуру гладкого (или топологического) многообразия и найдите его размерность. Должно получиться $k(n-k)$, где $n = \dim V$.

Предложение 8.18. *Имеет место* вложение Плюккера

$$\mathrm{Gr}(k, V) \hookrightarrow \mathbb{P}\Lambda^k V, \qquad \langle u_1, \dots, u_k\rangle \mapsto [u_1 \wedge \dots \wedge u_k].$$

Его образ задается однородными алгебраическими уравнениями в $\mathbb{P}\Lambda^k V$.

Доказательство. Теорема 8.15 показывает, что это отображение действительно корректно определено (при замене базиса в подпространстве соответствующий поливектор умножается на скаляр) и является вложением (это в точности часть (2) теоремы).

Докажем, что его образ задается алгебраическими уравнениями. Для этого нам понадобится следующая лемма.

Лемма 8.19. *Пусть* $\omega \in \Lambda^k V$ *— произвольный поливектор. Рассмотрим отображение* $\Phi_\omega \colon V \to \Lambda^{k+1} V$, $v \mapsto v \wedge \omega$. *Тогда* $\dim \operatorname{Ker} \Phi_\omega \leq k$, *причем равенство достигается тогда и только тогда, когда* ω *разложи́м.*

Доказательство. Выберем в V базис $e_1, \dots, e_n$ так, чтобы первые r его векторов образовывали базис в $\operatorname{Ker} \Phi_\omega$. Разложим ω по базису в $\Lambda^k V$:

$$\omega = \sum a_{i_1,\dots,i_k} e_{i_1} \wedge \dots \wedge e_{i_k} = \sum a_I e_I.$$

(I — это мультииндекс, то есть множество из k чисел от 1 до n).

Поскольку при $i \leq r$ вектор e_i лежит в ядре Φ_ω, то $\omega \wedge e_i = 0$, поэтому i лежит в каждом из множеств I. Значит, $\{1, \dots, r\} \subset \bigcap_{a_I \neq 0} I$. Поэтому $r \leq k$, причем равенство достигается тогда и только тогда, когда в ω только одно слагаемое, т.е. ω разложим. □

Итак, условие разложимости поливектора ω равносильно тому, что $\dim \operatorname{Ker} \Phi_\omega \geq k$, или, что то же самое, $\operatorname{rk} \Phi_\omega \geq n - k$. Это условие задается обращением в нуль всех миноров порядка $n - k + 1$ матрицы отображения Φ_ω, а это набор однородных уравнений на

коэффициенты ω. Поэтому $\mathrm{Gr}(k, V) \subset \mathbb{P}\Lambda^k V$ задается однородными алгебраическими уравнениями, или, что то же самое, является проективным алгебраическим многообразием. □

Эти уравнения имеют достаточно большую степень. Оказывается, впрочем, что для задания грассманиана можно обойтись и квадратичными уравнениями, так называемыми *соотношениями Плюккера*. Мы выведем эти уравнения лишь в специальном случае, когда $k = 2$.

8.7. Критерий разложимости бивектора. Соотношения Плюккера для $\mathrm{Gr}(2, V)$. Начнем со следующей леммы, которая представляет и самостоятельный интерес.

Лемма 8.20. *Бивектор $\omega \in \Lambda^2 V$ является разложимым тогда и только тогда, когда $\omega \wedge \omega = 0$.*

Доказательство. Часть "только тогда" очевидна. Докажем часть "тогда". Будем вести доказательство по индукции по $n = \dim V$.

База: $\dim V = 2$, и все бивекторы пропорциональны $e_1 \wedge e_2$, то есть являются разложимыми.

Переход. Выберем в V базис $e_1, \ldots, e_n$. Пусть $\tilde{V} = \langle e_1, \ldots, e_{n-1} \rangle$. Представим ω в виде $\omega = \omega' + v \wedge e_n$, где $\omega' \in \Lambda^2 \tilde{V}$, $v \in \tilde{V}$. Тогда

$$0 = \omega \wedge \omega = (\omega' + v \wedge e_n) \wedge (\omega' + v \wedge e_n) = \omega' \wedge \omega' + 2\omega' \wedge v \wedge e_n.$$

Поскольку первое слагаемое не зависит от e_n, а второе зависит, то оба слагаемых равны нулю:

$$\omega' \wedge \omega' = 0, \qquad \omega' \wedge v = 0.$$

По предположению индукции, ω' разложим. Пусть $\omega' = x \wedge y$. Поскольку $\omega' \wedge v = 0$, то v является линейной комбинацией x и y. Пусть $v = \lambda x + \mu y$. Тогда легко видеть, что

$$\omega = (x - \mu e_n) \wedge (y + \lambda e_n).$$

□

Пусть $\omega = \sum_{i<j} p_{ij} e_i \wedge e_j$. Запишем условие $\omega \wedge \omega = 0$ в координатах:

$$\omega \wedge \omega = (\sum_{i<j} p_{ij} e_i \wedge e_j) \wedge (\sum_{k<l} p_{kl} e_k \wedge e_l) =$$
$$= 2 \sum_{i<j<k<l} (p_{ij}p_{kl} - p_{ik}p_{jl} + p_{il}p_{jk}) e_i \wedge e_j \wedge e_k \wedge e_l.$$

Итак, условие $\omega \wedge \omega = 0$ равносильно тому, что

$$p_{ij}p_{kl} - p_{ik}p_{jl} + p_{il}p_{jk} = 0, \qquad 1 \leq i < j < k < l \leq n. \qquad (*)$$

Эти уравнения называются *соотношениями Плюккера*. Мы доказали следующее предложение.

Предложение 8.21. *Уравнения* $(*)$ *задают грассманиан* $\mathrm{Gr}(k, V)$ *в пространстве* $\mathbb{P}\Lambda^2 V$.

Особенно просто это выглядит, когда $\dim V = 4$: в этом случае имеется лишь одно уравнение.

Следствие 8.22. *Грассманиан* $\mathrm{Gr}(2, 4) \subset \mathbb{P}\Lambda^2 V \cong \mathbb{P}^5$ *задается уравнением*

$$p_{12}p_{34} - p_{13}p_{24} + p_{14}p_{23} = 0.$$

Он является невырожденной квадратичной гиперповерхностью в $\mathbb{P}^5$.

Это соотношение напоминает *теорему Птолемея* из школьного курса планиметрии:

Теорема 8.23 (Птолемей, I век н.э.). *Пусть* $ABCD$ *— вписанный четырехугольник. Тогда на длины его сторон и диагоналей имеется соотношение*

$$AB \cdot CD - AC \cdot BD + AD \cdot BC = 0.$$

9. Девятая лекция, 4 июня 2013 г.

9.1. Эрмитово пространство. [1] Ранее мы уже имели дело с евклидовыми пространствами. Если на вещественном векторном пространстве задана положительно определенная симметрическая билинейная форма, то при помощи такой формы можно задать норму на V по правилу $\|v\| = (v,v)^{1/2}$ и измерять длины векторов, углы между ними и т.д.

Если же пространство V комплексное, то, как легко видеть, на V не бывает положительно определенных билинейных форм. Действительно, пусть задана такая форма, для которой $(v,v) > 0$ при $v \neq 0$. Тогда $(iv, iv) = i^2(v,v) = -(v,v) < 0$ — противоречие. Поэтому для введения нормы на комплексном векторном пространстве применяются *полуторалинейные* формы.

9.2. Полуторалинейные формы.

Определение 9.1. Пусть V — комплексное векторное пространство. Отображение $\alpha\colon V \times V \to \mathbb{C}$ называется *полуторалинейной формой* на V, если:

- оно линейно по второму аргументу: $\alpha(v, w+w') = \alpha(v,w) + \alpha(v,w')$; $\alpha(v, \lambda w) = \lambda \cdot \alpha(v,w)$;
- оно *антилинейно* по первому аргументу: $\alpha(v+v', w) = \alpha(v',w) + \alpha(v,w)$; $\alpha(\lambda v, w) = \overline{\lambda} \cdot \alpha(v,w)$.

В конечномерном случае полуторалинейную форму можно задать матрицей: пусть $e_1, \dots, e_n$ — некоторый базис пространства V. Пусть $A = (a_{ij})$, где $a_{ij} = \alpha(e_i, e_j)$. Тогда если $v = \sum x_i e_i$, $w = \sum y_j e_j$, то

$$\alpha(v,w) = \sum_{i,j} a_{ij} \overline{x_i} y_j.$$

9.3. Эрмитовы формы. Наша следующая задача — выяснить, что будет аналогом *симметрической* билинейной формы. Ее определение тоже оказывается нужно “подправить". Так, например, у полуторалинейной формы нельзя просто поменять местами аргументы: по нашему определению форма $\tilde{\alpha}(v,w) := \alpha(w,v)$ уже не будет полуторалинейной формой, т.к. она будет линейна по *первому* аргументу и антилинейна по *второму*. Чтобы получить полуторалинейную форму, результат надо еще сопрячь.

Определение 9.2. Полуторалинейная форма называется *эрмитовой*, если $\alpha(v,w) = \overline{\alpha(w,v)}$.

[1] Первая половина девятой лекции была посвящена грассманианам, плюккеровым соотношениям и т.п. Эта часть (будет) включена в записки восьмой лекции. Здесь только вторая половина лекции, про эрмитовы пространства.

Отсюда, в частности, следует, что для эрмитовой формы $\alpha(v,v) = \overline{\alpha(v,v)} \in \mathbb{R}$. А вещественные числа уже бывают положительными или отрицательными. Поэтому возникает следующее

Определение 9.3. Эрмитова форма α называется *положительно определенной*, если $\alpha(v,v) > 0$ при $v \neq 0$. Пространство, снабженное положительно определенной эрмитовой формой, называется *эрмитовым* (или *унитарным*).

Пример 9.4. На $\mathbb{C}^n$ существует каноническая положительно определенная эрмитова форма

$$(x,y) = \overline{x_1}y_1 + \cdots + \overline{x_n}y_n.$$

Пример 9.5. Рассмотрим пространство интегрируемых *комплекснозначных* функций на отрезке $[0,1]$ (или каком-нибудь еще множестве). На этом пространстве существует положительно определенная эрмитова форма, определенная по правилу

$$(f,g) = \int_0^1 \overline{f(x)}g(x)dx.$$

Упражнение 9.6. Проверьте, что в эрмитовом случае из любого базиса можно сделать ортонормированный при помощи верхнетреугольной замены (ортогонализация Грама–Шмидта).

9.4. Норма на эрмитовом пространстве. Пусть V — эрмитово пространство Введем на V норму по правилу $\|v\| = (v,v)^{1/2} \in \mathbb{R}_+$.

Упражнение 9.7. Докажите, что это действительно норма (в частности, для нее имеет место неравенство Коши–Буняковского–Шварца).

Как и в евклидовом случае, по норме можно восстановить скалярное произведение. Действительно, из равенств

$\|v+w\|^2 = \|v\|^2+\|w\|^2+2\,\mathrm{Re}(v,w)$ и $\|v+iw\|^2 = \|v\|^2+\|w\|^2-2i\,\mathrm{Im}(v,w)$

следует, что

$$(v,w) = \frac{1}{2}\left[\|v+w|^2 - |v+iw\|^2\right]$$

(проверьте это!).

10. Десятая лекция, 6 июня 2013 г.

В этой лекции через V будет обозначаться n-мерное *эрмитово* пространство, т.е. комплексное векторное пространство, на котором задана положительно определенная эрмитова форма $(\ ,\ )$.

10.1. Соответствие между V и V^*. С помощью формы $(\ ,\ )$ можно задать изоморфизм между пространством V и двойственным к нему V^*. А именно, при этом изоморфизме вектор v будет переходить в линейный функционал ξ_v, заданный по правилу:

$$\xi_v(w) := (v, w) \in \mathbb{C}$$

Этот функционал действительно будет линеен, поскольку форма $(\ ,\ )$ линейна по второму аргументу.

Мы получили отображение из V в V^*. Оно будет изоморфизмом *вещественных* векторных пространств; однако оно будет *антилинейно* по отношению к умножению на комплексные числа:

$$\lambda \cdot v \mapsto \xi_{\lambda v} = \overline{\lambda} \cdot \xi_v.$$

10.2. Соответствие между полуторалинейными формами и линейными операторами. Пусть $\mathcal{A}$ — линейный оператор на V. Он задает на V полуторалинейную форму $\varphi_{\mathcal{A}}(v, w)$ по правилу:

$$\varphi_{\mathcal{A}}(v, w) := (v, \mathcal{A}w).$$

Заметим, что, хотя форма $(\ ,\ )$ была эрмитовой, про форму $\varphi_{\mathcal{A}}$ этого утверждать нельзя: она, вообще говоря, эрмитовой не будет.

Пусть $\{e_1, \ldots, e_n\}$ — *ортонормированный* базис пространства V. Тогда матрица формы $\varphi_{\mathcal{A}}$ в этом базисе выглядит так же, как матрица $A = (a_{ij})$ оператора $\mathcal{A}$. Действительно,

$$\varphi_{\mathcal{A}}(e_i, e_j) = (e_i, \mathcal{A}e_j) = (e_i, \sum_k a_{kj} e_k) = a_{ij}.$$

Определим на пространстве полуторалинейных форм инволюцию (т.е. отображение, квадрат которого равен тождественному) по правилу:

$$\varphi(v, w) \mapsto \overline{\varphi(w, v)}.$$

(за счет сопряжения полученная форма снова будет полулинейна по первому аргументу и линейна по второму). Неподвижные точки этой инволюции — это в точности эрмитовы формы.

Поскольку формы можно отождествить с линейными операторами, мы получаем инволюцию на пространстве линейных операторов, называемую *сопряжением*: $\mathcal{A} \mapsto \mathcal{A}^*$. Согласно вышесказанному, сопряженный к $\mathcal{A}$ оператор — это оператор $\mathcal{A}^*$, удовлетворяющий равенству

$$(\mathcal{A}^* v, w) = (v, \mathcal{A}w) \qquad \forall v, w \in V.$$

Матрица $\mathcal{A}^*$ получается из матрицы $\mathcal{A}$ композицией транспонирования и комплексного сопряжения: $A^* = \overline{A^t}$.

10.3. Эрмитовы и косоэрмитовы операторы.

Определение 10.1. Оператор $\mathcal{A}$ называется *эрмитовым* (соотв. *косоэрмитовым*), если $\mathcal{A} = \mathcal{A}^*$ (соотв. $\mathcal{A} = -\mathcal{A}^*$).

Эрмитовы и косоэрмитовы операторы иногда еще называют *самосопряженными* и *антисамосопряженными*.

Предложение 10.2. *Эрмитовы и косоэрмитовы операторы образуют* вещественные *векторные пространства (обозначим их* $\mathrm{Herm}(V)$ *и* $\mathrm{SkewHerm}(V)$*). Пространство* $\mathrm{End}(V)$ *есть прямая сумма этих двух подпространств (т.е. всякий оператор есть сумма эрмитова и косоэрмитова). Размерности (вещественные!) этих подпространств равны* n^2.

Доказательство. Во-первых, ясно, что сумма двух (косо)эрмитовых операторов снова (косо)эрмитова, а при умножении на вещественный (но не комплексный!) скаляр (косо)эрмиров оператор снова остается таковым. Далее, если оператор одновременно эрмитов и косоэрмитов, то он нулевой, т.к. $\mathcal{A} = \mathcal{A}^* = -\mathcal{A}^*$. Поэтому эрмитовы и косоэрмитовы операторы образуют вещественные подпространства, пересекающиеся лишь по нулю.

Далее, пусть $\mathcal{A} \in \mathrm{End}(V)$ — произвольный оператор. Тогда операторы $\frac{1}{2}(\mathcal{A} + \mathcal{A}^*)$ и $\frac{1}{2}(\mathcal{A} - \mathcal{A}^*)$ будут эрмитовым и косоэрмитовым соответственно, а их сумма равна $\mathcal{A}$. Стало быть, $\mathrm{End}(V) = \mathrm{Herm}(V) \oplus \mathrm{SkewHerm}(V)$. Наконец, отображение $\mathcal{A} \mapsto i\mathcal{A}$ переводит эрмитовы операторы в косоэрмитовы и наоборот, задавая изоморфизм между (вещественными!) векторными пространствами $\mathrm{Herm}(V)$ и $\mathrm{SkewHerm}(V)$. Поэтому размерность каждого из них равна $\frac{1}{2}\dim_{\mathbb{R}} \mathrm{End}(V)$, т.е. n^2. □

Замечание 10.3. Про разложение оператора в сумму эрмитова и косоэрмитова можно думать как про обобщение разложения комплексного числа в сумму вещественного и чисто мнимого (а в случае $\dim V = 1$ это в точности одно и то же).

10.4. Унитарные операторы. Понятие унитарного оператора в эрмитовом пространстве является аналогом понятия ортогонального оператора в евклидовом пространстве.

Определение 10.4. Оператор $\mathcal{A}$ называется *унитарным*, если он сохраняет норму вектора: $||\mathcal{A}v|| = ||v||$ для любого $v \in V$.

Замечание 10.5. Оператор унитарен тогда и только тогда, когда он сохраняет скалярное произведение:

$$(\mathcal{A}v, \mathcal{A}w) = (v, w) \qquad \forall v, w \in V.$$

Действительно, импликация "только тогда"очевидна, а "тогда"следует из того, что скалярное произведение можно восстановить по норме.

Кроме того, унитарные операторы всегда невырождены, т.к. они не имеют ядра (в противном случае мы получили бы, что $||\mathcal{A}v|| = 0$ при ненулевом векторе $v \in \operatorname{Ker}\mathcal{A}$). Далее, произведение двух унитарных операторов и обратный к унитарному оператору снова унитарны. Поэтому унитарные операторы образуют группу, которая обозначается через $\mathrm{U}(V)$ и называется *унитарной группой*.

Предложение 10.6. *Унитарные операторы — это в точности операторы, удовлетворяющие условию $\mathcal{A}^{-1} = \mathcal{A}^*$.*

Доказательство. Пусть $u, v \in V$ — произвольные векторы. Тогда

$$(u, v) = (\mathcal{A}u, \mathcal{A}v) = (\mathcal{A}^*\mathcal{A}u, v).$$

Поэтому $\mathcal{A}\mathcal{A}^* = \mathcal{E}$, что равносильно тому, что $\mathcal{A}^{-1} = \mathcal{A}^*$. □

Множество матриц, удовлетворяющих условию $A^{-1} = A^*$, образует подгруппу в $\mathrm{GL}_n(\mathbb{C})$, которая обозначается через U_n и тоже называется унитарной группой.

Упражнение 10.7 (для тех, кто знает, что такое гладкое многообразие). Докажите, что U_n является *вещественным* гладким многообразием размерности n^2 в $2n^2$-мерном пространстве $\mathrm{Mat}_n(\mathbb{C})$.

Пример 10.8. $U_1 = \{z \in \mathbb{C} \mid z^{-1} = \overline{z}\}$ есть единичная окружность в $\mathbb{R}^2 \cong \mathbb{C}$.

10.5. Диагонализуемость и собственные значения.

Теорема 10.9. *Пусть $\mathcal{A}$ — оператор одного из трех типов: эрмитов, косоэрмитов или унитарный. Тогда*

(1) *Если подпространство $U \subset V$ является $\mathcal{A}$-инвариантным, то $U^\perp$ тоже $\mathcal{A}$-инвариантно.*
(2) *Оператор $\mathcal{A}$ диагонализуем в ортонормированном базисе.*
(3) *Если $\mathcal{A}$ эрмитов (соотв. косоэрмитов, унитарен), то все его собственные значения вещественны (соотв. чисто мнимые, равны по модулю 1).*

Доказательство. (1) доказывается примерно одинаково во всех трех случаях. Проведем самое сложное из трех рассуждений, для унитарного оператора $\mathcal{A}$.

Итак, докажем, что $\mathcal{A}U^\perp \subset U^\perp$. Возьмем произвольный вектор $w \in U^\perp$ и докажем, что $\mathcal{A}w \in U^\perp$, то есть что $(\mathcal{A}w, u) = 0$ для любого $u \in U$. Оператор $\mathcal{A}$, ограниченный на U, также будет унитарным, а следовательно, невырожденным. Стало быть, вектор $\widetilde{u} = \mathcal{A}u \in U$ отличен от нуля. Векторы $\widetilde{u}$ и w ортогональны. Поэтому

$$0 = (w, \widetilde{u}) = (\mathcal{A}w, \mathcal{A}\widetilde{u}) = (\mathcal{A}w, \mathcal{A}\mathcal{A}^{-1}u) = (\mathcal{A}w, u).$$

(во втором равенстве мы воспользовались ортогональностью $\mathcal{A}$). Поэтому $\mathcal{A}w \in U^\perp$, что и требовалось доказать. Случай эрмитова и косоэрмитова операторов разбираются аналогично (проделайте это сами).

(2) доказывается по индукции. При $\dim V = 1$ доказывать нечего. Докажем индуктивный переход: пусть $\dim V = n$. Поскольку $\mathcal{A}$ — оператор на комплексном векторном пространстве, у него есть собственный вектор $v \in V$. Будем считать, что $\|v\| = 1$. Тогда подпространство $U = \langle v \rangle^\perp$ тоже $\mathcal{A}$-инвариантно в силу пункта (1). Поэтому, согласно предположению индукции, в U существует ортонормированный базис $u_1, \dots, u_{n-1}$, в котором $\mathcal{A}$ диагонален. Но тогда $\mathcal{A}$ диагонален в базисе $u_1, \dots, u_{n-1}, v$ пространства V.

Докажем (3) это для эрмитова оператора. Пусть $\mathcal{A}v = \lambda v$. Тогда $\lambda(v,v) = (v, \lambda v = (v, \mathcal{A}v) = (\mathcal{A}v, v) = (\lambda v, v) = \overline{\lambda}(v,v)$, откуда $\lambda = \overline{\lambda} \in \mathbb{R}$. Случаи унитарного и косоэрмитова операторов разбираются аналогично. □

10.6. Полярное разложение.

Определение 10.10. Эрмитов оператор $\mathcal{A}$ называется положительно определенным, если все его собственные значения больше нуля.

Предложение 10.11 (об извлечении корня из положительно определенного эрмитова оператора). *Пусть $\mathcal{A}$ — положительно определенный эрмитов оператор. Тогда существует единственный положительно определенный эрмитов оператор $\mathcal{B}$, для которого $\mathcal{A} = \mathcal{B}^2$.*

Доказательство. Существование: пусть $\lambda_1, \dots, \lambda_k$ — различные собственные значения $\mathcal{A}$, $V_1, \dots, V_k$ — соответствующие им собственные подпространства (т.е. $\mathcal{A}|_{V_i} = \lambda_i \mathcal{E}$). Пусть $\mu_i = \sqrt{\lambda_i} > 0$. Определим оператор $\mathcal{B}$, действующий на каждом из V_i умножением на μ_i. Ясно, что $\mathcal{B}^2 = \mathcal{A}$.

Докажем единственность. Пусть $\mathcal{B}$ — искомый оператор. Он диагонализуем; пусть W_i — его собственные подпространства, отвечающие собственным значениям μ_i. Тогда пространства W_i будут собственными и для оператора $\mathcal{A} = \mathcal{B}^2$, который будет действовать на каждом из W_i умножением на μ_i^2. Отсюда следует, что набор W_i получается из набора V_i подходящей перенумерацией, т.е. $\mathcal{B}$ определен однозначно. □

Лемма 10.12. *Пусть $\mathcal{A}$ — произвольный невырожденный оператор. Тогда оператор $\mathcal{A}\mathcal{A}^*$ — положительно определенный эрмитов.*

Доказательство. Эрмитовость очевидна: $(\mathcal{A}\mathcal{A}^*)^* = \mathcal{A}^{**}\mathcal{A}^* = \mathcal{A}\mathcal{A}*$. Для доказательства положительной определенности заметим,

что если $v \in V$ — собственный вектор $\mathcal{A}\mathcal{A}^*$, отвечающий собственному значению $\lambda \neq 0$, $\lambda \in \mathbb{R}$,

$$\lambda = (\lambda v, v)/(v, v) = (\mathcal{A}\mathcal{A}^* v, v)/(v, v) = (\mathcal{A}^* v, \mathcal{A}^* v)/(v, v) = \|\mathcal{A}^* v\|^2/\|v\|^2 > 0.$$

□

Сформулируем и докажем теорему о полярном разложении оператора, которая является аналогом представления комплексного числа в тригонометрической форме: $z = re^{i\varphi}$, где $r > 0$, $e^{i\varphi} = 1$.

Теорема 10.13 (о полярном разложении). *Всякий невырожденный линейный оператор $\mathcal{A}$ можно представить в виде $\mathcal{A} = \mathcal{B}\mathcal{C}$, где $\mathcal{B}$ — положительно определенный эрмитов оператор, $\mathcal{C}$ — унитарный оператор, причем это представление единственно.*

Доказательство. Сначала докажем единственность: что если такое представление существует, то $\mathcal{B}$ и $\mathcal{C}$ определены однозначно. Итак, пусть $\mathcal{A} = \mathcal{B}\mathcal{C}$, где $\mathcal{B} = \mathcal{B}^*$, а $\mathcal{C}\mathcal{C}^* = \mathcal{E}$. Тогда по предыдущей лемме оператор $\mathcal{A}\mathcal{A}^* = \mathcal{B}\mathcal{C}\mathcal{C}^*\mathcal{B}^* = \mathcal{B}\mathcal{B}^* = \mathcal{B}^2$ — положительно определенный эрмитов. Значит, из него в силу предложения 10.11 единственным образом извлекается корень, т.е. оператор $\mathcal{B}$ определен однозначно. Но тогда и $\mathcal{C}$ определен однозначно, т.к. $\mathcal{C} = \mathcal{B}^{-1}\mathcal{A}$.

Докажем существование. Рассмотрим положительно определенный эрмитов оператор $\mathcal{A}\mathcal{A}^*$. Из него извлекается корень: пусть $\mathcal{B}$ таков, что $\mathcal{A}\mathcal{A}^* = \mathcal{B}^2$. Тогда положим $\mathcal{C} = \mathcal{B}^{-1}\mathcal{A}$. Тогда $\mathcal{A} = \mathcal{B}\mathcal{C}$, а $\mathcal{A}\mathcal{A}^* = \mathcal{B}\mathcal{C}\mathcal{C}^*\mathcal{B} = \mathcal{B}^2$, откуда $\mathcal{C}\mathcal{C}^* = \mathcal{E}$. Стало быть, $\mathcal{C}$ унитарен. Теорема доказана. □

E-mail address: evgeny.smirnov@gmail.com