Независимый Московский Университет

Алгебра

Первый курс, весенний семестр 2004/05 г.
Лекции 3–4

Простейшие классификационные теоремы линейной алгебры

Пусть $\Bbbk$ — поле. Я предполагаю известными понятия векторного пространства над $\Bbbk$, линейной зависимости, базиса, размерности, линейного отображения. Также я буду пользоваться тем, что любое линейно независимое семейство векторов в конечномерном векторном пространстве можно дополнить до базиса.

Основная задача линейной алгебры — задача классификации (с точностью до изоморфизма). Простейшим примером такой классификации является

Теорема 1. *Любое конечномерное векторное пространство V над $\Bbbk$ изоморфно $\Bbbk^n$ для некоторого n, причем пространства $\Bbbk^n$ и $\Bbbk^m$ неизоморфны при $n \neq m$.*

Из этой теоремы следует, что размерность является единственным инвариантом конечномерных векторных пространств.

Будем рассматривать пары (U, V), где $U \subseteq V$. Назовем две пары $(U_1, V_1) \simeq (U_2, V_2)$ *изоморфными*, если существует изоморфизм $\varphi: \quad V_1 \to V_2$, такой что $\varphi(U_1) = U_2$.

Пусть $(u_1, \ldots, u_k)$ — базис U. Дополним его до базиса пространства V векторами $v_1, \ldots, v_l$. Пусть $n = \dim V = k + l$ и $(e_1, \ldots, e_n)$ — базис $\Bbbk^n$. Тогда $\Bbbk^k$ — линейная оболочка первых k элементов этого базиса. Легко видеть, что $(\Bbbk^k, \Bbbk^n) \simeq (U, V)$:

$$\varphi(e_i) = \begin{cases} u_i, & i \leqslant k \\ v_{i-k}, & i > k. \end{cases}$$

Получилась

Теорема 2. *Любая пара (U, V), где V — конечномерное векторное пространство над $\Bbbk$, а $U \subseteq V$ — его подпространство, изоморфна паре вида $(\Bbbk^k, \Bbbk^n)$ для некоторых n и $k \leqslant n$.*

Пусть U и W — подпространства конечномерного векторного пространства V. Изоморфизмы троек (U, W, V) определяются аналогично тому, как определялись изоморфизмы пар (U, V).

Рассмотрим подпространство $U \cap W = \langle v_1, \ldots, v_k \rangle$, где $v_1, \ldots, v_k$ — его базис. Дополним его до базисов подпространств U и W векторами $v_{k+1}, \ldots, v_l$ и $v_{l+1}, \ldots, v_m$ соответственно. Пусть векторы линейно зависимы, т.е. $\sum\limits_{i=1}^{m} \alpha^i v_i = 0$, где α^i не все равны нулю. Тогда, очевидно,

$$\sum_{i=1}^{k} \alpha^i v_i + \sum_{i=k+1}^{l} \alpha^i v_i = -\sum_{i=l+1}^{m} \alpha^i v_i.$$

Вектор, стоящий в левой части равенства, лежит в U, а вектор, стоящий в правой части, — в W, а, значит, он принадлежит их пересечению. Следовательно, $\sum\limits_{i=l+1}^{m} \alpha^i v_i = \sum\limits_{j=1}^{k} \beta^j v_j$, а значит, $\alpha^i = 0 \quad \forall i \in \{l+1, \ldots, m\}$. Поэтому $\sum\limits_{i=1}^{k} \alpha^i v_i + \sum\limits_{i=k+1}^{l} \alpha^i v_i = 0$, и $\alpha^i = 0 \quad \forall i \in \{1, \ldots, l\}$ (так как $v_1, \ldots, v_l$ — базис U). Итак, $V = \langle v_1, \ldots, v_m \rangle$, то есть для любых двух подпространств конечномерного векторного пространства можно выбрать базис, согласованный с этой парой подпространств.

Сформулируем соответствующую классификационную теорему (несколько в ином стиле, чем две предыдущие).

Теорема 3. *Конечномерное пространство V и два его подпространства U и W определяются однозначно (с точностью до изоморфизма) следующими четырьмя инвариантами: $k = \dim V$, $l = \dim U$, $m = \dim W$ и $n = \dim(U \cap W)$, которые могут принимать любые неотрицательные целые значения, удовлетворяющие неравенствам $n \leqslant m \leqslant k$ и $n \leqslant l \leqslant k$.*

Еще один пример классификационной задачи — закон инерции.

Определение 1. *Билинейной формой* на пространстве V над полем $\Bbbk$ называется функция $b : V \times V \to \Bbbk$, линейная по каждой переменной. Билинейная форма b называется *симметрической*, если $b(v_1, v_2) = b(v_2, v_1)$ для любых $v_1, v_2 \in V$. *Квадратичной формой*, ассоциированной с билинейной формой b, называется функция $q : V \to \Bbbk$, заданная формулой $q(v) = b(v, v)$. Квадратичная форма над полем $\mathbb{R}$ называется *положительно определенной*, если $q(v) > 0$ для любого $v \neq 0$.

Отметим, что если характеристика поля $\Bbbk$ не равна 2, то для определения квадратичной формы достаточно рассматривать только симметрические билинейные формы (при замене $b(v_1, v_2)$ на $(b(v_1, v_2) + b(v_2, v_1))/2$ квадратичная форма не меняется); к тому же симметрическую билинейную форму можно восстановить по ассоциированной с ней квадратичной с помощью *поляризации*: $b(v_1, v_2) = (q(v_1 + v_2) - q(v_1) - q(v_2))/2$.

Определение 2. Матрица $A = (a_{ij})$ билинейной формы b в базисе $e_1, \ldots, e_n$ определяется равенством $a_{ij} = b(e_i, e_j)$.

В координатах билинейная форма вычисляется так: $b\left(\sum_i x_i e_i, \sum_j y_j e_j\right) = \sum_{i,j} a_{ij} x_i y_j$. При замене базиса с матрицей C матрица билинейной формы преобразуется в $C^t A C$ (проверьте).

Теорема 4 (Закон инерции). *Заменой базиса матрицу симметрической билинейной формы можно привести к диагональному виду. Если поле $\Bbbk$ алгебраически замкнуто, то можно добиться того, чтобы на диагонали стояли только единицы и нули, причем количество единиц определено однозначно. Если $\Bbbk = \mathbb{R}$, то можно считать, что на диагонали стоят только 1, -1 и 0, причем количество 1 (положительный индекс инерции), количество -1 (отрицательный индекс инерции) и количество 0 определены однозначно.*

Доказательство. Возможность привести матрицу к требуемому виду доказывается легко (проделайте это). Инвариантность числа единиц в случае алгебраически замкнутого поля следует из того, что ранг матрицы A не меняется при заменах базиса. В более инвариантных терминах — назовем ядром билинейной формы b множество тех $v \in V$, для которых $b(v, u) = 0$ при любом $u \in V$. Легко проверить, что ядро является линейным подпространством пространства V, и его размерность в случае диагональной матрицы формы — это число нулей на диагонали.

В случае $\Bbbk = \mathbb{R}$, рассмотрим квадратичную форму q, ассоциированную с b. Проверьте, что положительнй индекс инерции — это максимально возможная размерность подпространства, на котором форма q положительно определена. Отсюда легко следует инвариантность индексов инерции. $\square$

Рассмотрим, в чем состоит общий подход к задаче классификации.

Пусть нам надо классифицировать векторные пространства с некоторой дополнительной структурой (парой подпространств, или квадратичной формой, или чем-то ещё). Обозначим пространство V с этой дополнительной структурой через $\mathbf{V}$ и назовём *объектом*.

В любой классификационной задаче есть понятие изоморфизма объектов $\mathbf{V} \cong \mathbf{W}$. Обычно это просто линейный изоморфизм, «согласованный с дополнительной структурой». Определение согласованности, как правило, не вызывает затруднений.

Полное решение задачи классификации — это:

1) список *стандартных объектов* $\mathbf{V}_s$, где s пробегает некоторое множество индексов, такой, что любой объект $\mathbf{V}$ изоморфен ровно одному из объектов V_s;

2) список *инвариантов* φ_r, каждый из которых сопоставляет объекту $\mathbf{V}$ некоторое число $\varphi_r(\mathbf{V})$, такой, что $\mathbf{V} \cong \mathbf{W}$ тогда и только тогда, когда $\varphi_r(\mathbf{V}) = \varphi_r(\mathbf{W})$ для любого r.

Заметим, что выбор базиса в n-мерном пространстве V — это не что иное как выбор изоморфизма $\Bbbk^n \to V$. Таким образом, в случае пространств с квадратичной формой, закон инерции дает нам как список стандартных объектов ($\Bbbk^n$ с формой, заданной диагональной матрицей стандартного вида), так и (для $\Bbbk = \mathbb{R}$ или $\Bbbk$ алгебраически замкнутого) полный набор инвариантов.

Для получения полного списка стандартных объектов очень полезен следующий подход.

Пусть V и W — векторные пространства. Их *прямой суммой* $V \oplus W$ называется множество всевозможных пар (v, w), где $v \in V$, $w \in W$. На $V \oplus W$ вводится структура векторного пространства: $(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2)$ и $\lambda(v, w) = (\lambda v, \lambda w)$.

Если каждое из пространств V и W снабжено нашей «дополнительной структурой», то (для всех рассматривавшихся классификационных задач) на прямой сумме $V \oplus W$ тоже возникает естественная дополнительная структура. Например, если в пространствах V и W заданы подпространства V_0 и W_0 соответственно, то в $V \oplus W$ возникает подпространство $V_0 \oplus W_0$, и т. п. Таким образом, мы получаем понятие *прямой суммы объектов* $\mathbf{V} \oplus \mathbf{W}$.

Операция взятия прямой суммы объектов является коммутативной и ассоциативной (в смысле изоморфизма соответствующих прямых сумм; например, коммутативность — это изоморфизм $\mathbf{V} \oplus \mathbf{W} \cong \mathbf{W} \oplus \mathbf{V}$).

Объект $\mathbf{V}$ называется нулевым, если соответствующее векторное пространство V является нулевым. Объект $\mathbf{V}$ называется неразложимым, если он не изоморфен никакой прямой сумме ненулевых объектов.

Ясно, что любой ненулевой объект изоморфен прямой сумме нескольких неразложимых. Поэтому важной составной частью задачи классификации является нахождение всех (с точностью до изоморфизма) неразложимых объектов.

Упражнение 1. Докажите, что в задачах классификации пространств с k выделенными подпространствами ($k = 0, 1, 2$) каждый неразложимый объект представляют собой одномерное пространство (каждое из выделенных подпространств либо одномерно, либо нульмерно).

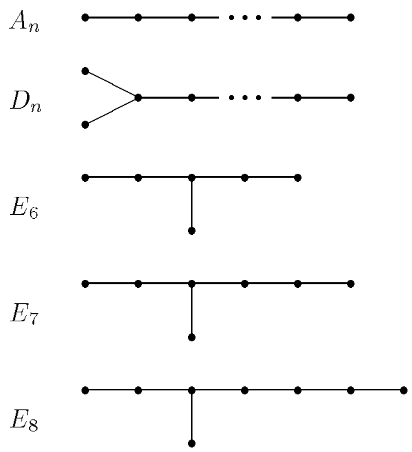

Рис. 1.

Упражнение 2. Найдите неразложимые объекты в задаче классификации пространств с квадратичной формой над $\mathbb{R}$.

Список всех неразложимых объектов особенно полезен тогда, когда для каждого объекта любое его разложение в прямую сумму неразложимых содержит одни и те же слагаемые (с точностью до перестановки).

Упражнение 3. Проверьте, что во всех рассматривавшихся ранее задачах классификации это так.

Рассмотрим еще один тип классификационных задач.

Назовём *колчаном* произвольный ориентированный граф. *Представлением колчана над полем* $\Bbbk$ называется следующий набор данных: для каждой вершины i — некоторое конечномерное векторное пространство V_i над $\Bbbk$, а для каждой стрелки e из i в j — линейное отображение $\varphi_e : V_i \to V_j$. Представления (V_i, φ_e) и (W_i, ψ_e) данного колчана называются изоморфными, если для каждой вершины i колчана существует изоморфизм $f_i : V_i \to W_i$, причем $f_j \varphi_e = \psi_e f_i$ для любой стрелки из i в j.

Прямой суммой представлений (V_i, φ_e) и (W_i, ψ_e) данного колчана называется представление $(V_i \oplus W_i, \varphi_e \oplus \psi_e)$, где $\varphi_e \oplus \psi_e$ — отображение, переводящее каждую пару (v, w) в пару $(\varphi_e v, \psi_e w)$.

Колчаны, представления которых имеют «простую» классификацию, описываются знаменитой теоремой Габриэля. Часть утверждений этой теоремы можно сформулировать так:

Теорема 5. *Колчан Γ имеет лишь конечное число неизоморфных неразложимых представлений над $\mathbb{R}$ тогда и только тогда, когда каждая связная компонента Γ получается некоторой расстановкой стрелок в одном из графов на рис. 1 (графы Кокстера; ADE-классификация). При этом набор неразложимых представлений, на которые раскладывается данное представление, определяется этим представлением однозначно.*

Вместо полного доказательства этой теоремы (которого я и сам не знаю), я примерно обЪясню как здесь вообще возникают графы Кокстера.

Обозначим вершины графа Γ натуральными числами от 1 до n. Ясно, что достаточно рассмотреть связные колчаны.

Размерность пространства $\mathcal{V}(d_1, \ldots, d_n)$ всех представлений колчана, для которых $V_i = \mathbb{R}^{d_i}$, равна, очевидно, $\sum_{e \in E} d_{i(e)} d_{j(e)}$, где E — множество стрелок колчана, а через $i(e)$ и $j(e)$ обозначены, соответственно, начало и конец стрелки e. Если число неизоморфных неразложимых представлений конечно, то конечно и число всех неизоморфных представлений с данным набором размерностей $d_1, \ldots, d_n$ пространств, отвечающих вершинам колчана. Это последнее число равно, очевидно, числу орбит группы $GL(d_1, \mathbb{R}) \times \cdots \times GL(d_n, \mathbb{R})$, действующей на пространстве $\mathcal{V}(d_1, \ldots, d_n)$ по формулам замены базиса: $(g_1, \ldots, g_n)\varphi_e = g_{j(e)}^{-1} \varphi_e g_{i(e)}$. Размерность каждой из орбит не больше $\sum_{i=1}^n d_i^2 - 1$ (так как стабилизатор каждой точки $\mathcal{V}(d_1, \ldots, d_n)$ содержит одномерную подгруппу, состоящую из элементов вида $(\lambda, \ldots, \lambda) \in GL(d_1, \mathbb{R}) \times \cdots \times GL(d_n, \mathbb{R})$). Поскольку пространство $\mathcal{V}(d_1, \ldots, d_n)$ покрыто конечным числом таких орбит, его размерность не может быть больше максимально возможной размерности орбиты, то есть функция $f(d_1, \ldots, d_n) = \sum_{i=1}^n d_i^2 - \sum_{e \in E} d_{i(e)} d_{j(e)}$ должна принимать положительное значение на любом ненулевом наборе неотрицательных целых чисел. Отсюда легко следует, что эта функция положительна на любом ненулевом наборе целых чисел, а следовательно и на любом ненулевом наборе рациональных (и даже действительных) чисел. Доказательство того, что все связные графы, для которых квадратичная форма f положительно определена, описываются ADE-классификацией, я оставляю в качестве упражнения (не очень простого).

Вышеприведенное рассуждение опирается на понятие размерности многообразия и на тот факт, что образ многообразия при гладком отображении не может покрыть многообразие большей размерности (это следует, например, из теоремы Сарда). Надеюсь, что всё это вы рано или поздно изучите в курсе математического анализа.

Классификация пространств с k выделенными подпространствами практически эквивалентна классификации представлений колчана из k стрелок, ведущих в одну вершину из k других. Из теоремы Габриэля следует, что простая классификация есть при $k \leq 3$. Классификация пространств с тройкой подпространств также оставляется в качестве упражнения.

Двойственное линейное пространство

Подпространство линейного пространства V можно задавать как линейную оболочку некоторого семейства элементов пространства V. Очевидно, что любое подпространство конечномерного линейного пространства можно получить как линейную оболочку конечного семейства векторов (кстати, почему это очевидно?).

С другой стороны, подпространства можно задавать линейными уравнениями.

Определение 3. *Линейной функцией* на линейном пространстве V называется любое линейное отображение $\xi : V \to \Bbbk$. Множество V^* всех линейных функций на V обладает естественной структурой линейного пространства. Это пространство называется *двойственным* к V.

Утверждение 1. *Пусть V — конечномерное линейное пространство над полем $\Bbbk$. Тогда двойственное пространство V^* тоже конечномерно, и $\dim V^* = \dim V$.*

Доказательство. Пусть $\dim V = n$ и $(e_1, \ldots, e_n)$ — базис пространства V. Определим линейные функции $\varepsilon_1, \ldots, \varepsilon_n \in V^*$ как координатные функции относительно базиса $(e_1, \ldots, e_n)$, то есть для любого вектора $v = \sum x_i e_i$ мы положим $\varepsilon_j(v) = x_j$. Поскольку разложение вектора по базису определено однозначно, то функции $\varepsilon_1, \ldots, \varepsilon_n$ определены корректно; линейность их также не вызывает сомнений. Докажем, что $(\varepsilon_1, \ldots, \varepsilon_n)$ — базис пространства V^*.

Очевидно, что функции $\varepsilon_1, \ldots, \varepsilon_n$ являются линейно независимыми. С другой стороны, по определению линейности, для любой функции $\xi \in V^*$ имеет место равенство: $\xi(\sum x_i e_i) = \sum x_i \xi(e_i)$, то есть $\xi = \sum \xi(e_i)\varepsilon_i$. Поэтому $V^* = \langle \varepsilon_1, \ldots, \varepsilon_n \rangle$. Итак, $(\varepsilon_1, \ldots, \varepsilon_n)$ — базис пространства V^*, и $\dim V^* = \dim V$. □

Базис $(\varepsilon_1, \ldots, \varepsilon_n)$ называется *двойственным* к базису $(e_1, \ldots, e_n)$. Отметим, что он однозначно определяется условием $\varepsilon_i(e_j) = \delta_{ij}$.

Любой вектор $v \in V$ определяет линейную функцию $\xi \mapsto \xi(v)$ на пространстве V^*, то есть элемент дважды двойственного пространства $(V^*)^*$. Легко видеть, что при $\dim V < \infty$ мы получаем канонический (то есть не зависящий от выбора базиса) изоморфизм $V \to (V^*)^*$. Впредь мы будем отождествлять любое конечномерное пространство с дважды двойственным к нему.

Казалось бы, ничто не мешает отождествить пространство V и с V^* с помощью изоморфизма, переводящего базис (e_i) в базис (ε_i). Однако этот изоморфизм зависит от выбора базиса (e_i).

Действительно, пусть (e_i') — другой базис пространства V. Рассмотрим матрицу $A \in M_{n\times n}$, j-тый столбец которой составляют координаты вектора e_j' в базисе (e_i) $(j = 1, \ldots, n)$. Эта матрица называется *матрицей перехода* от базиса (e_i) к базису (e_i'). Пусть e — строка $(e_1, \ldots, e_n)$, а e' — строка $(e_1', \ldots, e_n')$. Имеет место следующее матричное равенство: $e' = eA$ (по определению матрицы A).

Пусть $x = (x_1, \ldots, x_n)$ — строка координат вектора $v \in V$ в базисе e, а $x' = (x_1', \ldots, x_n')$ — строка координат того же вектора в базисе e'. Положим $X = x^t$ и $X' = (x')^t$ — те же координаты, записанные в столбец. Тогда $v = eX = e'X'$. Отсюда $X = AX'$. Транспонируя, получаем $x = x'A^t$, или $x' = x(A^t)^{-1}$. Последнее равенство, верное для любого вектора $v \in V$, мы можем интерпретировать как правило пересчета координатных функций, связанных с базисом e, в координатные функции, связанные с базисом e'. Другими словами, имеет место матричное рвенство $\varepsilon' = \varepsilon(A^t)^{-1}$, где $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n)$ — базис V^*, двойственный к базису e, а $\varepsilon' = (\varepsilon_1', \ldots, \varepsilon_n')$ — базис V^*, двойственный к базису e'. Итак, матрицей перехода от базиса ε к базису ε' является $(A^t)^{-1}$. Таким образом, наше отождествление V с V^* выдерживает не все замены базиса, а лишь те, для которых $A = (A^t)^{-1}$. Такие матрицы называются ортогональными. Другое их описание — это матрицы, сохраняющие стандартное евклидово произведение в $\Bbbk^n$ (билинейную форму, заданную единичной матрицей.) Действительно, билинейную форму на V можно воспринимать как линейное отображение $V \to V^*$ (подставив вектор в билинейную форму,олучаем линейную функцию.) Матрица формы в базисе e — это матрица соответствующего линейного отображения $V \to V^*$ относительно базисов e и ε. Поэтому рассмотренное выше отождествление V с V^* отвечает стандартному евклидову произведению в базисе e.

Пусть задано линейное отображение (оператор) $F : V \to W$. По любой функции $\xi : W \to \Bbbk$ мы можем построить функцию на $F^*\xi : W \to \Bbbk$, положив $F^*\xi(v) = \xi(Fv)$. Ясно, что если ξ — линейная функция, то и $F^*\xi$ — линейная функция, и что отображение $F^* : W^* \to V^*$ является линейным. Оно называется *сопряженным линейным отображением* (или *сопряженным оператором*) к F.

Легко проверить, что для любого оператора $F : V \to W$ выполнено равенство $F^{**} = F$ (напомню, что мы рассматриваем только конечномерные векторные пространства и отождествляем каждое пространство с дважды двойственным к нему).

Упражнение 4. Доказать, что

1) если $F : V \to W$ — изоморфизм векторных пространств, то $F^* : W^* \to V^*$ — тоже изоморфизм;

2) если $G : U \to V$ и $F : V \to W$ — произвольные линейные отображения, то $(FG)^* = F^*G^*$.

Определение 4. Пусть V — векторное пространство над полем $\Bbbk$. *Аннулятором* подпространства $U \subseteq V$ называется подпространство $U^\circ \subseteq V^*$, состоящее из всех линейных функций на V, обращающихся тождественно в нуль на подпространстве U.

То, что мы отождествили V^{**} с V, позволяет нам рассматривать аннулятор любого подпространства $W \subseteq V^*$ как подпространство пространства V.

Утверждение 2. *Для любого подпространства $U \subseteq V$ выполнено равенство $U^{\circ\circ} = U$.*

Доказательство. Воспользуемся классификацией подпространств (теорема 2). Выберем в V базис $(v_1, \dots, v_n)$, согласованный с подпространством U (то есть такой, что $U = \langle v_1, \dots v_k \rangle$). Пусть $(v_1^*, \dots, v_n^*)$ — двойственный базис пространства V^*. Тогда, очевидно, $U^\circ = \langle v_{k+1}^*, \dots, v_n^* \rangle$ и $U^{\circ\circ} = \langle v_1, \dots v_k \rangle = U$. □

Аналогично, с использованием классификации линейных отображений, доказывается

Утверждение 3. *Для любого линейного отображения $F : V \to W$ выполнены равенства:*

$$(\operatorname{Ker} F)^\circ = \operatorname{Im} F^* \qquad \text{и} \qquad (\operatorname{Im} F)^\circ = \operatorname{Ker} F^*.$$

Утверждение 2 означает, по существу, что любое подпространство U пространства V можно задать системой линейных уравнений на координаты вектора (эти уравнения соответствуют элементам пространства U°). Более того, достаточно взять $\dim U^\circ$ уравнений, отвечающих элементам произвольного базиса этого пространства. Число $\dim U^\circ = \dim V - \dim U$ называется *коразмерностью* подпространства U в пространстве V и обозначается $\operatorname{codim} U$.

Определение 5. Подпространства $V_1, \dots, V_n \subseteq V$ являются *линейно независимыми*, если из равенства $v_1 + \dots + v_n = 0$ ($v_i \in V_i$) следует, что $v_1 = \dots = v_n = 0$.

Для двух подпространств V_1 и V_2 линейная независимость равносильна тому, что $V_1 \cap V_2 = 0$. Легко проверить, что для большего числа подпространств это неверно.

Определение 6. *Суммой* подпространств $U_1, \dots, U_n \in V$ называется совокупность векторов вида $u_1 + \dots + u_n$, где $u_i \in U_i$. Сумма называется *прямой* (и обозначается $V_1 \oplus \dots \oplus V_n$), если подпространства линейно независимы.

Алгебры

Определение 7. *Алгеброй над полем* $\Bbbk$ называется кольцо A, являющееся одновременно линейным пространством над полем $\Bbbk$, в котором кольцевые операции согласованы со структурой линейного пространства, то есть сложение – общее и $\alpha(ab) = (\alpha a)b = a(\alpha b)$ для любых $a, b \in A$ и $\alpha \in \Bbbk$. Другими словыми, умножение в алгебре является билинейным отображением $A \times A \to A$.

Определение 8. *Левым модулем над ассоциативной алгеброй с единицей* A называется векторное пространство V, элементы которого можно умножать слева на элементы алгебры, причем умножение $A \times V \to V$ является билинейным.

Пример 1. Поле комплексных чисел $\mathbb{C}$ является алгеброй размерности два над полем вещественных чисел $\mathbb{R}$. Любое поле характеристики p является алгеброй над полем $\mathbb{F}_p$ (по существу, мы уже пользовались этим, когда доказывали, что любое конечное поле характеристики p имеет p^k элементов). Кольцо многочленов $\Bbbk[x]$ является бесконечномерной алгеброй над полем $\Bbbk$.

Модуль над полем — это то же самое, что векторное пространство над полем.

Упражнение 5. Доказать, что кольцо M_n матриц $n \times n$ над полем $\Bbbk$ является алгеброй размерности n^2 над полем $\Bbbk$, а арифметическое векторное пространство $\Bbbk^n$ является модулем над алгеброй M_n.

Кольцо многочленов можно определить не только над полем, но и над произвольным коммутативным кольцом. В частности, можно рассмотреть кольцо многочленов над $\Bbbk[x]$. Получается $\Bbbk[x, y] = \Bbbk[x][y]$ — *кольцо многочленов от двух переменных*. Легко видеть, что $\Bbbk[x, y]$ является алгеброй над $\Bbbk$ с базисом, состоящем из *мономов* $x^k y^l$, где $k, l \in \mathbb{N} \cup \{0\}$.

Аналогично определяется алгебра $\Bbbk[x_1,\ldots,x_n]$ многочленов от n переменных; базис ее над $\Bbbk$ составляют мономы $x_1^{k_1}\ldots x_n^{k_n}$.

Пусть $(a_1,\ldots,a_n)$ — базис алгебры A над полем $\Bbbk$ как линейного пространства. Из определения ясно, что структура алгебры однозначно определяется произведениями базисных элементов a_ia_j для всех $i,j\in\{1,\ldots,n\}$. Поскольку $(a_1,\ldots,a_n)$ — базис, эти произведения можно по нему разложить:

$$a_ia_j=\sum_{k=1}^{n}c_{ij}^k a_k.$$

Элементы $c_{ij}^k\in\Bbbk$ называются *структурными константами* алгебры A. Отметим, что произвольный выбор структурных констант определяет на линейном пространстве A структуру алгебры, которая, вообще говоря, не будет ни коммутативной, ни ассоциативной.

Упражнение 6. При каком условии на структурные константы c_{ij}^k алгебра A является коммутативной? Ассоциативной?

Пример 2. Определим алгебру кватернионов $\mathbb{H}$ как линейное пространство над $\mathbb{R}$ с базисом $(1,i,j,k)$, где произведения базисных векторов определяются так:

$$\begin{aligned}
1\cdot 1=-i\cdot i=-j\cdot j=-k\cdot k &= 1;\\
1\cdot i=i\cdot 1=j\cdot k=-k\cdot j &= i;\\
1\cdot j=j\cdot 1=k\cdot i=-i\cdot k &= j;\\
1\cdot k=k\cdot 1=i\cdot j=-j\cdot i &= k.
\end{aligned}$$

Алгебра $\mathbb{H}$, очевидно, не является коммутативной.

Утверждение 4. *Алгебра $\mathbb{H}$ является ассоциативной.*

Доказательство: Доказать ассоциативность алгебры $\mathbb{H}$ можно прямой проверкой. Мы поступим чуть-чуть иначе.

Рассмотрим в алгебре матриц $M_4(\mathbb{R})$ линейное подпространство H, состоящее из матриц вида

$$\begin{pmatrix} a & -b & -c & -d\\ b & a & -d & c\\ c & d & a & -b\\ d & -c & b & a\end{pmatrix}.$$

Базис H составляют матрицы

$$E=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\qquad I=\begin{pmatrix}0&-1&0&0\\1&0&0&0\\0&0&0&-1\\0&0&1&0\end{pmatrix},$$

$$J=\begin{pmatrix}0&0&-1&0\\0&0&0&1\\1&0&0&0\\0&-1&0&0\end{pmatrix}\quad\text{и}\quad K=\begin{pmatrix}0&0&0&-1\\0&0&-1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}.$$

Непосредственно проверяется, что эти матрицы удовлетворяют соотношениям

$$\begin{aligned}
E\cdot E=-I\cdot I=-J\cdot J=-K\cdot K &= E;\\
E\cdot I=I\cdot E=J\cdot K=-K\cdot J &= I;\\
E\cdot J=J\cdot E=K\cdot I=-I\cdot K &= J;\\
E\cdot K=K\cdot E=I\cdot J=-J\cdot I &= K.
\end{aligned}$$

Отсюда следует, что, во-первых, H замкнуто относительно умножения, то есть является подалгеброй алгебры $M_4(\mathbb{R})$, и, во-вторых, алгебра H изоморфна алгебре кватернионов $\mathbb{H}$. Ассоциативность алгебры $\mathbb{H}$ следует теперь из ассоциативности умножения матриц. $\square$

Определение 9. В произвольном ассоциативном кольце R с единицей элемент $a\in R$ называется *обратимым*, если существует $b\in R$, для которого $ab=ba=1$.

Ассоциативное кольцо R с единицей называется *телом*, если каждый ненулевой элемент $a\in R$ обратим.

Легко видеть, что обратимые элементы произвольного ассоциативного кольца с единицей образуют группу по умножению.

Утверждение 5. *Алгебра $\mathbb{H}$ является телом.*

Доказательство: Пусть $h=a+bi+cj+dk\in\mathbb{H}$. Положим $\overline{h}=a-bi-cj-dk\in\mathbb{H}$. Тогда $h\overline{h}=\overline{h}h=a^2+b^2+c^2+d^2$ и если $h\neq 0$, то $\overline{h}/(a^2+b^2+c^2+d^2)$ является обратным к h. $\square$

Алгебра Грассмана

Алгебра Грассмана от n переменных над полем $\Bbbk$, построение которой будет изложено далее, является ассоциативной алгеброй с единицей. Она почти столь же важна в математике, как и кольцо многочленов от нескольких переменных, и во многом аналогична ему. Кольцо многочленов $\Bbbk[x_1, \ldots, x_n]$ порождено набором коммутирующих переменных $(x_1, \ldots, x_n)$, между которыми нет других соотношений. Алгебра Грассмана $\Lambda^\bullet(\xi^1, \ldots, \xi^n)$ порождена набором *антикоммутирующих* переменных $\xi^1, \ldots, \xi^n$, между которыми также нет других соотношений.

Слово «антикоммутирующие» означает следующее: $\xi^i \wedge \xi^j = -\xi^j \wedge \xi^i$ для любых $i, j \in [1, n]$, а также $\xi^i \wedge \xi^i = 0$ для любого $i \in [1, n]$ (где $[1, n]$ обозначает множество целых чисел от 1 до n). При $\operatorname{char} \Bbbk \neq 2$ второе условие следует из первого. Знак $\wedge$ в алгебре Грассмана традиционно используется для обозначения произведения. Умножение в алгебре Грассмана называется *внешним умножением*.

Условие антикоммутативности умножения на первый взгляд сильно отличается от коммутативности, но на самом деле ничем не хуже — оно позволяет переставлять в любом произведении $\xi^{i_1} \wedge \cdots \wedge \xi^{i_k}$ соседние сомножители местами, при этом произведение просто меняет знак. Отсюда следует, что в алгебре Грассмана любое произведение образующих либо равно нулю, либо равно, с точностью до знака, произведению образующих со строго возрастающими номерами. Поэтому каждый элемент алгебры Грассмана линейно выражается через такие произведения.

Все вышесказанное представляет собой только наводящие соображения — алгебру Грассмана еще предстоит построить. Дадим точные определения.

Зафиксируем набор *грассмановых переменных* $\xi^1, \ldots, \xi^n$. *Грассмановым мономом* от $\xi^1, \ldots, \xi^n$ называется выражение вида $\xi^{i_1} \wedge \cdots \wedge \xi^{i_k}$, где $1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n$. Обозначим такой моном через ξ^I, где $I = \{i^1, \ldots, i^k\}$. Таким образом, грассмановы мономы находятся во взаимно однозначном соответствии с подмножествами множества $\{1, \ldots, n\}$. Пустому множеству при этом соответствует произведение пустого множества образующих, то есть 1.

Положим $\xi^{i_{\sigma(1)}} \wedge \cdots \wedge \xi^{i_{\sigma(k)}} = \varepsilon(\sigma)\xi^{i_1} \wedge \cdots \wedge \xi^{i_k}$ для любой перестановки $\sigma \in S_k$ (напомню, что через $\varepsilon(\sigma)$ обозначается знак перестановки σ). Произведение $\xi^{j_1} \wedge \cdots \wedge \xi^{j_m}$, где среди набора индексов $(j_1, \ldots, j_m)$ есть повторяющиеся, положим равным нулю.

Теперь легко определить произведение $\xi^I \wedge \xi^J$ грассмановых мономов ξ^I и ξ^J. Оно получается просто приписыванием одного монома к другому через знак $\wedge$ и преобразованием получившегося выражения по изложенным выше правилам. Результат можно описать так:

$$\xi^I \wedge \xi^J = \begin{cases} 0, & \text{если } I \cap J \neq \varnothing, \\ (-1)^{c(I,J)}\xi^{I \cup J}, & \text{если } I \cap J = \varnothing, \end{cases}$$

где

$$c(I, J) = \#\{(i, j) \in I \times J \mid i > j\}.$$

(Знак $\#$ обозначает число элементов множества.)

Упражнение 7. Доказать, что введенное умножение мономов является ассоциативным.

Обозначим через $\Lambda^\bullet(\xi^1, \ldots, \xi^n)$, или просто через $\Lambda^\bullet$, линейное пространство над полем $\Bbbk$ с базисом (ξ^I), то есть пространство всех выражений вида

$$\sum_{I \subseteq [1,n]} a_I \xi^I,$$

где $a_I \in \Bbbk$. Введенное на базисе этого пространства умножение задает структуру алгебры на $\Lambda^\bullet$. По построению это алгебра с единицей. Легко видеть, что ассоциативность умножения в алгебре достаточно проверять на базисе (см. упражнение 6). Из упражнения 7 получаем, что алгебра $\Lambda^\bullet$ является ассоциативной. Она и называется алгеброй Грассмана.

Размерность алгебры Грассмана равна числу всех подмножеств множества $[1, n]$, то есть $\dim \Lambda^\bullet = 2^n$. Назовем *степенью* монома $\xi^{i_1} \wedge \cdots \wedge \xi^{i_k}$ число k. Грассмановы мономы степени k образуют базис подпространства $\Lambda^k \subseteq \Lambda^\bullet$. Ясно, что $\dim \Lambda^k = \binom{n}{k}$ и $\Lambda^\bullet = \bigoplus\limits_{k=0}^{n} \Lambda^k$. Отметим также, что при перемножении степени мономов складываются.

Пусть $\alpha, \beta \in \Lambda^1$, то есть $\alpha = \sum\limits_{i=1}^{n} a_i \xi^i$ и $\beta = \sum\limits_{i=1}^{n} b_i \xi^i$. Тогда, как легко убедиться, $\alpha \wedge \alpha = 0$ и $\alpha \wedge \beta = -\beta \wedge \alpha$. Эти равенства понадобятся нам на следующей лекции.

Упражнение 8. Доказать, что если $\zeta \in \Lambda^p$ и $\eta \in \Lambda^q$, то

$$\zeta \wedge \eta = (-1)^{pq} \eta \wedge \zeta.$$

Замечание. Определитель $\det A$ матрицы $A = (a^i_j) \in M_n(\Bbbk)$ может быть определен как коэффициент при $\xi^1 \wedge \cdots \wedge \xi^n$ в произведении n грассмановых полиномов первой степени

$$\Big(\sum_{j=1}^{n} a^1_j \xi^j\Big) \wedge \Big(\sum_{j=1}^{n} a^2_j \xi^j\Big) \wedge \cdots \wedge \Big(\sum_{j=1}^{n} a^n_j \xi^j\Big) = (\det A)\xi^1 \wedge \cdots \wedge \xi^n.$$