Оглавление

0.1. Определение алгебры кватернионов...

Определение алгебры кватернионов. Векторное произведение. Сопряжённый кватернион. Норма кватерниона. Мультипликативность нормы. Сумма четырёх квадратов.

Наша цель сейчас рассказать про геометрию трехмерного пространства используя при этом определённые алгебраические конструкции. А именно, ещё в XIX веке Уильям Роуэн Гамильтон стал искать аналогичную комплексным числам алгебраическую систему на трёхмерном пространстве. Однако, подходящий аналог удалось найти только в четырёхмерной ситуации.

Рассмотрим подпространство в алгебре матриц $M_2(\mathbb{C})$ вида

$$\mathbb{H} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \right\}.$$

Базис этого пространства, как вещественного векторного пространства, состоит из матриц

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Для этого достаточно показать их линейную независимость и замкнутость относительно сложения. Второе очевидно, для первого, например, заметим, что никакая нетривиальная линейная комбинация первых двух матриц не может занулить оба элемента на главной диагонали, а две других матрицы не содержат элементов на главной диагонали. Аналогично для двух правых матриц.

Покажем, что это вещественная подалгебра в $M_2(\mathbb{C})$ и следовательно ассоциативное кольцо.

Ассоциативность умножения следует из определения в виде подпространства матриц.

Далее достаточно показать, что произведение базисных снова лежит в $\mathbb{H}$. Имеем

$$i^2 = j^2 = k^2 = -1 \text{ и } ij = k = -ji,$$

, проверяется прямым умножением матриц. Отсюда получаем

$$ik = i(k) = i(ij) = (ii)j = -j = j(-1) = j(ii) = (ji)i = (-k)i = -ki \text{ и } jk = -jjk = -i = -kj.$$

Таким образом $\mathbb{H}$ образует ассоциативную алгебру размерности 4 над $\mathbb{R}$.

Определение (Алгебра кватернионов)**.** $\mathbb{H}$ называется алгеброй кватернионов.

В дальнейшем будем рассматривать кватернионы как формальные суммы $a + bi + cj + dk$ с верными доказанными выше тождествами.

Определение (Вещественная и мнимая часть)**.** Вещественная или скалярная часть кватерниона $\operatorname{Re} x = a$, мнимая или векторная часть $v = \operatorname{Im} x = bi + cj + dk$.

Определение (Векторное произведение)**.** Пусть $u = (a, b, c), v = (a', b', c') \in \mathbb{R}^3$ два вектора. Тогда их векторным произведением называется вектор $[u, v]$, задаваемый по формуле

$$[u, v] = (bc' - cb')i + (ca' - ac')j + (ab' - ba')k = \begin{vmatrix} i & j & k \\ a & b & c \\ a' & b' & c' \end{vmatrix}$$

Замечание. Операция $(u, v) \to [u, v]$ является билинейной (проверяется по определению) и антисимметричной (в каждой скобке в определении векторного произведения меняется знак), получаем $[u, u] = 0$ и $[u, v] = -[v, u]$.

Определение (Чисто мнимый кватернион)**.** Кватернион называется чисто мнимым, если его вещественная часть равна нулю. Часто обычный кватернион будем обозначать в виде $a+u$, где u — чисто мнимый.

Рассмотрим произведение двух чисто мнимых кватернионов $u=(ai+bj+ck)$ и $v=(a'i+b'j+c'k)$
$uv=-(aa'+bb'+cc')+(bc'-cb')i+(ca'-ac')j+(ab'-ba')k=-\langle u,v\rangle+[u,v]$.

Определение (Сопряжённый кватернион)**.** Пусть x — кватернион, $x=a+bi+cj+dk=a+u$. Сопряжённым кватернионом называется $\overline{x}=a-bi-cj-dk=\operatorname{Re}x-\operatorname{Im}x=a-u$.

Замечание. $x\overline{x}=(a+u)(a-u)=a^2-u^2=a^2+\langle u,u\rangle-[u,u]=a^2+(b^2i+c^2j+d^2k)-0=\overline{x}x$

Определение (Норма кватерниона)**.** Определим норму кватерниона как

$$||x||=\sqrt{x\overline{x}}=\sqrt{a^2+b^2+c^2+d^2}=\sqrt{\overline{x}x}.$$

Замечание. Все необходимые свойства нормы проверяются напрямую

Норма кватерниона, как и модуль комплексного числа всегда положительны для ненулевых элементов. Это позволяет заметить, что

Определение (Обратный кватернион)**.** Если $0\neq x\in\mathbb{H}$, то $x^{-1}=\frac{\overline{x}}{||x||^2}$.

Поскольку $xx^{-1}=\frac{x\overline{x}}{||x||^2}=1$

Таким образом мы получили первый (и для нас единственный) пример некоммутативного кольца с делением. Такие кольца называются телами. Напоминаю, что алгебра для нас ассоциативна и с единицей.

Замечание. Связь между матричным и стандартным определением кватернионов
Пусть $v=\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}$,тогда $u=\begin{pmatrix}a+bi & c+di\\ -c+di & a-bi\end{pmatrix}=a+bi+cj+dk$
$\det v=\alpha\overline{\alpha}+\beta\overline{\beta}=a^2+b^2+c^2+d^2$
Отсюда $||x||=\sqrt{\det x}$

Лемма 1 (Норма мультипликативна)**.** $||xy||=||x||\,||y||$ и $||x^{-1}||=||x||^{-1}$.

Доказательство. $||xy||=\sqrt{\det x}\sqrt{\det y}=\sqrt{\det x\det y}=\sqrt{\det xy}$, т.к. определитель мультипликативен.
Отсюда, $||x||\,||x^{-1}||=||xx^{-1}||=||1||=1$

□

Отойдём немного в сторону и посмотрим на первое внутриалгебраическое применение кватернионов. Довольно давно был поставлен вопрос, какие натуральные числа бывают суммой четырёх квадратов. Лагранжем было доказано, что любое натуральное число допускает такое представление. Доказательство можно условно разбить на два этапа:
1) Показать такое представление для любого простого p.
2) Свести случай произвольного числа к случаю простого.

Мы не будем касаться первого пункта (см. Теорема Лагранжа). Разберёмся со вторым пунктом. Сначала докажем лемму

Лемма 2 (Сумма четырёх квадратов)**.** В кольце целых чисел произведение $(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2)$ снова есть сумма четырёх квадратов (а на самом деле и в любом коммутативном кольце с 1).

Доказательство. Пусть $n_1=a^2+b^2+c^2+d^2, n_2=e^2+f^2+g^2+h^2$, заметим, что $n_1=||a+bi+cj+dk||^2, n_2=||e+fi+gj+hk||^2$. По мультипликативности нормы $n_1n_2=||(a+bi+cj+dk)(e+fi+gj+hk)||^2$. Легко заметить, что внутри получается некоторый кватернион с целыми коэффициентами (покуда каждый коэффициент является суммой произведения целых). Значит выражение будет равно сумме квадратов коэффициентов этого кватерниона.

Лемма 3 (Сведение произвольного числа к простому)**.** Если мы доказали теорему для простых чисел, и что если теорема верна для двух чисел, то верна и для их произведения, то поскольку любое целое число представимо в виде произведения простых, то теорема верна и для любого целого числа (например, по индукции).

0.2. Свойства сопряжения и векторного произведения.

Лемма 4. Отображение $x \to \overline{x}$ является антиизоморфизмом алгебр, то есть $\overline{ab} = \overline{b}\,\overline{a}$.

Доказательство. Линейность:
$\overline{x_1 + x_2} = \overline{(a+u) + (a'+u')} = \overline{(a+a') + (u+u')} = (a+a') - (u+u') = (a-u) + (a'-u') = \overline{a+u} + \overline{a'+u'}$
$\overline{kx_1} = \overline{k(a+u)} = \overline{ka + ku} = ka - ku = k(a-u) = k\overline{x_1}$

Далее пусть $x, y \neq 0$. Тогда
$\frac{\overline{y}\,\overline{x}}{||y||^2||x||^2} = y^{-1}x^{-1} = (xy)^{-1} = \frac{\overline{xy}}{||xy||^2}$, $\overline{y}\,\overline{x} = \overline{xy}$

Напоминание: $y^{-1}x^{-1}xy = 1 \to (xy)^{-1} = y^{-1}x^{-1}$

На самом деле и здесь можно было воспользоваться матричным представлением. А именно, можно заметить, что операция сопряжения совпадает на этом языке с транспонированием и сопряжением соответствующей комплексной матрицы.

Замечание. Если u чисто мнимый, то $u^2 = -\langle u, u\rangle + [u, u] = -\langle u, u\rangle = -||u||^2$

Замечание. $\langle x, y\rangle = \langle y, x\rangle$

Лемма 5 (Свойства векторного произведения)**.** Верны следующие свойства для чисто мнимых u, v
1) $u \perp [u, v]$. Точнее

$$u[u, v] = -||u||^2 v + \langle u, v\rangle\, u$$

2) $|||[u, v]||| = ||u||||v|||\sin\varphi|$, где φ – это угол между u и v.

Доказательство. .
1)
$u[u, v] = -\langle u, [u, v]\rangle + [u, [u, v]]$, с другой стороны
$u[u, v] = u(uv + \langle u, v\rangle) = u^2 v + \langle u, v\rangle\, u = -||u||^2 v + \langle u, v\rangle\, u$

Последнее выражение, очевидно, чисто мнимое, а значит скалярное произведение равно нулю, вектора перпендикулярны.

2)
$||[u, v]||^2 = -[u, v][u, v] = [u, v][v, u] = (uv + \langle u, v\rangle)(vu + \langle v, u\rangle) = (uv + \langle u, v\rangle)(vu + \langle u, v\rangle) = u(vv)u + \langle u, v\rangle^2 + \langle u, v\rangle\,(uv + vu) =$
Заметим, что $uv + vu = -\langle u, v\rangle - \langle v, u\rangle + [u, v] + [v, u] = -2\langle u, v\rangle + [u, v] - [u, v] = -2\langle u, v\rangle$
$= u||v||^2 u + \langle u, v\rangle^2 - 2\langle u, v\rangle^2 = ||u||^2||v||^2 - \langle u, v\rangle^2 = ||u||^2||v||^2(1 - \cos^2\varphi)$
В последнем мы пользуемся определением $cos\phi = \frac{\langle a,b\rangle}{||a||\,||b||}$ □

0.3. Кватернионы и...

Кватернионы и вращения R^3

Определение. Обозначим за $\mathbb{H}_1$ подгруппу кватернионов, по норме равных единице.

Замечание. Это действительно подгруппа по умножению вследствие мультипликативности нормы.

Теорема 1. Отображение $L : \mathbb{H}_1 \to \mathrm{GL}_3(\mathbb{R})$ заданное по правилу $x \to (y \to xyx^{-1})$ корректно определено и даёт сюръективный гомоморфизм из группы кватернионов единичной нормы в $\mathrm{SO}_3(\mathbb{R})$. Ядро этого гомоморфизма состоит из $\{\pm 1\}$. Точнее, если единичный кватернион x представим в виде $x = a + bv$, где v — чисто мнимый, $||v|| = 1$, то соответствующее вращение есть вращение относительно оси $\langle v\rangle$ на угол 2φ, где $\cos\varphi = a$, $\sin\varphi = b$ или тождественное преобразование в случае $v = \pm 1$.

Доказательство. Рассмотрим преобразование $L_x \colon \mathbb{H} \to \mathbb{H}$ вида $y \to xyx^{-1}$ Прежде всего покажем, что мы получили ортогональное преобразование $\mathbb{R}^4$, для этого нужно показать, что оно линейно и сохраняет норму.
$L_x(a + b) = x(a + b)x^{-1} = xax^{-1} + xbx^{-1}$
$L_x(ka) = xkax^{-1} = kxax^{-1} = kL_x$
$||xyx^{-1}|| = ||x||\,||y||\,||x^{-1}|| = ||y||\,||x||\,||x||^{-1} = ||y||$.

Теперь заметим, что преобразование L_x сохраняет на месте вектор 1: $x\,1\,x^{-1} = 1$. Следовательно, сохраняет его ортогональное дополнение, то есть $\mathbb{R}^3$. Таким образом L_x ограничивается на $\mathbb{R}^3$.

Гомоморфизм: $L_x L_y = yx\, v\, x^{-1}y^{-1} = L_{xy}$.

Тем самым мы доказали, что L — гомоморфизм и задаёт ортогональные преобразования в $\mathbb{R}^3$.

Ось вращения: заметим, что если $t = a + bv, t \in \mathbb{H}_1$, то L_t оставляет v на месте. Действительно, при $b \neq 0$
$tvt^{-1} = t(\frac{t-a}{b})t^{-1} = \frac{ttt^{-1} - tat^{-1}}{b} = \frac{t-a}{b} = v$.

Пусть теперь $v = (x, y, z) \in H_1$. Тогда заметим, что $1 = ||t||^2 = ||a + bv||^2 = a^2 + b^2(x^2 + y^2 + z^2) = a^2 + b^2||v||^2 = a^2 + b^2$
Отсюда $|a|, |b| \leq 1, a^2 + b^2 = 1 \to a = \cos\varphi, b = \sin\varphi$ для некоторого φ.

Рассмотрим нормированный вектор $u \perp v$ и $[v, u] \perp u$, которые образуют ортонормированный базис $\mathbb{R}^2$ дополнения и посчитаем tut^{-1} и $t[v, u]t^{-1}$.

Замечание. Если $x \perp y, x, y$ — чисто мнимые, то $xy = -\langle x, y\rangle + [x, y] = [x, y]$
Если $x \in H_1$, то $x^{-1} = \frac{\overline{x}}{||x||} = \overline{x}$
Если x чисто мнимый, то $x^2 = -\langle x, x\rangle + [x, x] = -||x||^2$
Если x чисто мнимый, то $||a + bx|| = a^2 + b^2||x||$ (доказано выше)

$tut^{-1} = (a + bv)u(a - bv) = (a + bv)(au - b[u, v]) = a^2u - ab[u, v] + ab[v, u] - b^2v[u, v] =$
$-v[u, v] = v[v, u] = vvu = -||v||^2u = -u$
$= a^2u + 2ab[v, u] - b^2u = (a^2 - b^2)u + 2ab[v, u]$
Заметим, что $a^2 - b^2 = \cos^2\varphi - \sin^2\varphi = \cos 2\varphi$
$2ab = \sin 2\varphi$
$u \to \cos 2\varphi\, u + \sin 2\varphi\, [v, u]$

$t[v, u]t^{-1} = (a + bv)[v, u](a - bv) = (a + bv)(vua + buvv) = (a + bv)([v, u]a - bu) = a^2[v, u] - b^2[v, u] - abu + abvvu = (a^2 - b^2)[v, u] - 2abu = -\sin 2\varphi u + \cos 2\varphi[v, u]$

Посмотрим на определитель матрицы перехода между базисами, он равен $\cos^2 2\varphi + \sin^2 2\varphi = 1$. Тем самым данное преобразование является поворотом по определению.

Посмотрим на cos угла между u и $L_t(u)$. По определению $\cos(u, L_t(u)) = \frac{\langle u, \cos 2\varphi\, u + \sin 2\varphi[v,u]\rangle}{||u||||\cos 2\varphi\, u + \sin 2\varphi||} = \frac{\langle u, \cos 2\varphi\, u\rangle + \langle u, \sin 2\varphi[v,u]\rangle}{||u(\cos 2\varphi\, u + \sin 2\varphi\, [v,u])||} = \frac{\cos 2\varphi\, ||u||^2}{||-\cos 2\varphi + \sin 2\varphi v||} = \frac{\cos 2\varphi}{\cos^2 2\varphi + \sin^2 2\varphi||v||} = \frac{\cos 2\varphi}{\cos^2 2\varphi + \sin^2 2\varphi} = \cos 2\varphi$

Тем самым вектор действительно повернулся на угол 2φ.

Наконец, сюръективность: пусть хотим поворот относительно оси t на угол 2φ. Сначала нормируем $t = \frac{t'}{||t||}$, затем берём $a = \cos\varphi, b = \sin\varphi$, тогда, по доказанному ранее, для $x = a + bt'$, L_x — искомый поворот.

По поводу $u = \pm 1$ заметим, что в таком случае $t = a + bu = \pm 1$ (t по норме равен 1 и чисто вещественный). В таком случае $\sin\varphi = \pm 1, 2\varphi = 0$ или 2π.

□

Данная задача не требуется в билете, но пусть будет.

Задача 1. Покажите, что отображение $(x, y) \to (z \to xzy^{-1})$ задаёт сюръективный гомоморфизм из декартового квадрата группы единичных кватернионов в группу $\mathrm{SO}_4(\mathbb{R})$ с ядром $\{(1, 1), (-1, -1)\}$.

На практике мы доказали TODO Написать доказательство, что $\forall f \in SO4$ имеет вид $f(x) = ax\overline{b}, ||a|| = ||b|| = 1$
Поэтому если взять отображение $H_1 \times H_1 \to SO4$ по правилу $(a, b) \to (x \to ax\overline{b})$ получим сюръективное отображение.
Проверим гомоморфизм, $f((a, b) \cdot (c, d)) = f(a \cdot c, b \cdot d) = (x \to ac\, x\, \overline{bd}) = (x \to ac\, x\, \overline{d}\ \overline{b}) = (x \to a(c\, x\, \overline{d})\overline{b}) = f(a, b) \circ f(c, d)$

Осталось найти ядро. $(a, b) : \forall x, ax\overline{b} = x$
$b, a \neq 0$ т.к. $b, a \in H_1$
$\overline{b} = b^{-1}$
Пусть $x = 1$, получаем $ab^{-1} = 1$
$a = b$

Но из лекции мы знаем, что отображение вида $x \to axa^{-1}, a \in H_1$ является гомоморфизмом с ядром ± 1, таким

образом ядром нашего отображения будет $(1,1)$ и $(-1,-1)$

0.4. Максимум квадратичной формы на сфере. Теорема Куранта-Фишера.

TODO: шпаргалка

Теперь обратимся к вопросам, связанным с вещественными самосопряжёнными операторами. Для этого заметим, что с каждым самосопряжённым оператором L на евклидовом пространстве можно связать билинейную симметричную форму $\langle x, Ly\rangle$ или, что эквивалентно, квадратичную форму $\langle x, Lx\rangle$. Безусловно по квадратичной форме можно обратно восстановить оператор.

Рассмотрим один из вопросов, связанных с такой конструкцией, а именно, рассмотрим задачу о нахождении нормы линейного оператора $L\colon U \to V$ между двумя евклидовыми пространствами. Для того, чтобы найти норму необходимо найти (по одному из определений нормы)

$$\max_{x\neq 0} \sqrt{\frac{\langle Lx, Lx\rangle}{\|x\|^2}} = \sqrt{\max_{x\neq 0} \frac{\langle L^*Lx, x\rangle}{\|x\|^2}} = \sqrt{\max_{\|x\|=1} \langle L^*Lx, x\rangle}.$$

Таким образом, нахождение нормы оператора свелось к задаче максимизации квадратичной формы на единичной сфере. Заметим, что максимум действительно достигается благодаря компактности сферы.

Оказывается, что довольно легко найти максимум или минимум квадратичной формы на сфере.

Теорема 2. Пусть V – евклидово пространство, A – самосопряжённый оператор на V, а $q(x) = \langle x, Ax\rangle$ – соответствующая квадратичная форма. Тогда

$$\max_{x\in V} \frac{q(x)}{||x||^2} = \max_{\substack{x\in V \\ ||x||=1}} q(x) = \lambda_1,$$

где λ_1 - наибольшее собственное число оператора A и достигается на собственном векторе v_1, соответствующему λ_1. Аналогично минимум равен минимальному собственному числу A.

Доказательство. Пусть $v = \sum c_i e_i$, причём $1 = ||v||^2 = \sum c_i^2$. Тогда $\langle Av, v\rangle = \sum c_i^2\lambda_i$, что меньше $\langle Ae_1, e_1\rangle = \lambda_1 = \sum c_i^2\lambda_1$ т.к. $\forall i, \lambda_i \leq \lambda_1$ по выбору λ_1. Доказательство для минимума полностью аналогично. □

Эта теорема, кроме, собственно, решения задачи, даёт геометрическую характеризацию первого собственного числа. Вопрос: можно ли аналогично охарактеризовать другие собственные числа? Ответ получается не таким простым, но, тем не менее, полезным.

Теорема 3 (Куранта-Фишера)**.** Пусть $q(x) = \langle x, Ax\rangle$. Тогда k-ое по убыванию собственное число λ_k для A есть

$$\lambda_k = \max_{\dim L=k} \min_{\substack{x\in L \\ ||x||=1}} q(x) = \min_{\dim L=n-k+1} \max_{\substack{x\in L \\ ||x||=1}} q(x).$$

Причем максимум достигается на инвариантном подпространстве, содержащем собственные вектора для $\lambda_1, \ldots, \lambda_k$.

Доказательство. Пусть U — подпространство на котором достигается максимум, причём допустим, что максимум больше λ_k. Тогда рассмотрим подпространство $W = \langle v_k, \ldots, v_n\rangle$, где v_i — собственный вектор соответствующий i-ому по убыванию собственному числу. Заметим, что $U \cap W = \{0\}$, так как на W форма принимает значения меньше или равные λ_k (смотри предыдущую теорему), а на U – строго большие. Однако $\dim W = n - k + 1$. Приходим к противоречию с подсчётом размерности пересечения.

Максимум достигается на подпространстве $w = \langle \lambda_1, \ldots, \lambda_k\rangle$, смотри предыдущую теорему.

Вторая формулировка данной теоремы доказывается полностью аналогично. □

0.5. Оценка на собственные числа ограничения. Оценка на след.

1. С.ч. операторов A и B. По КФ, мин/макс для μ_i берется по подпр. внутри соотв. подпр. для λ. 2. Это след: взять матрицу A в ортонорм. базисе u_i. $v_i = (0, \ldots, 1, \ldots, 0)^T$ $A_{i,i} = v_i^T A v_i = q(u_i)$. Оценка: почленные нер-ва из 1.

Теорема 4. Оценка на собственные числа ограничения

Пусть $q(x)$ — квадратичная форма на евклидовом пространстве V; $q(x) = x^T Ax$. $U \leq V$. Рассмотрим сужение q на U: $q|_U$. Тогда этой форме соответствует оператор B такой, что $q|_U = x^T Bx$. Обозначим собственные числа A как λ_i, при чём $\lambda_i \geq \lambda_{i+1}$. Аналогично собственные числа B — μ_j; $\mu_j \geq \mu_{j+1}$. Тогда выполняются неравенства:

$$\lambda_{i+n-m} \leq \mu_i \leq \lambda_i$$

Доказательство. $\mu_i \leq \lambda_i$

Пусть $dim\, U = m,\ dim\, V = n$. Тогда по теореме Куранта-Фишера:

$$\lambda_i = \max_{L \leq V,\, dim\, L = i} \min_{x \in L} q(x)$$

Такое же равенство для μ_i:

$$\mu_i = \max_{T \leq U,\, dim\, T = i} \min_{x \in T} q(x)$$

$T \leq U \leq V \Rightarrow\ T \leq V$. Значит, в равенстве для λ_i максимум берётся по всем подпространствам, которые учтены в μ_i и ещё каким-то $\Rightarrow \lambda_i \geq \mu_i$. Что и требовалось.

$\mu_i \geq \lambda_{i+n-m}$

Применим второе равенство из теоремы Куранта-Фишера.

$$\lambda_{i+n-m} = \min_{L \leq V,\, dim\, L = n-(i+n-m)+1 = m-i+1} \max_{x \in L} q(x)$$

$$\mu_i = \min_{T \leq U,\, dim\, T = m-i+1} \max_{x \in T} q(x)$$

По тем же соображениям $T \leq V$. В равенстве для λ_i минимум берётся по всем подпространствам, которые учтены в μ_i и ещё каким-то $\Rightarrow \lambda_{i+n-m} \leq \mu_i$. Что и требовалось.

□

Определение. След квадратичной формы

Пусть q — квадратичная форма на евклидовом пространстве V. u_i — ортонормированный базис V. Тогда определим след q следующим образом:

$$Tr\, q = \sum_{i=1}^{dim\, V} q(u_i)$$

Теорема 5. Это действительно след!

Если в базисе u_i форме $q(x) = x^T Ax$ соответствует симметричная матрица A, то $Tr\, q = Tr\, A$. И след квадратичной формы не зависит от выбора ортонормированного базиса.

Доказательство. Посчитаем след матрицы A в базисе u_i.

Как вычислить значение i-го диагонального элемента матрицы? Возьмём $v_i = (0, \dots, 1, \dots 0)$ (единица на v-ой позиции). Посчитаем $v_i A v_i^T$. Получим $A_{i,i}$. (Упражнение: убедиться, что это действительно так.)

Но $q(u_i) = (0, \dots, 1, \dots, 0)A(0, \dots, 1, \dots, 0)^T = v_i A v_i^T$.

След не зависит от выбора базиса, так как при переходе к новому базису у нас получится $Tr\, CAC^{-1}$, а последнее равно $Tr\, A$, так как $Tr(AB) = Tr(BA)$ (прошлый семестр) и C-шки умрут.

□

Теорема 6. Оценка на след

Пусть $U \leq V$, где V — евклидово, $dim\, V = n,\ dim\, U = m$. $q(x)$ — квадратичная форма на V. $q(x) \geq 0$ на всех x. Тогда:

$$Tr(q) \geq Tr(q|_U)$$

Доказательство. След оператора — сумма его собственных чисел. По неравенству $\lambda_i \geq \mu_i$ и неотрицательности q получаем $\sum_{i=1}^{n} \lambda_i \geq \sum_{i=1}^{m} \mu_i$, а это как раз следы соответствующих операторов (а они равны следам квадратичных форм).

Замечание. А в будущем потребуется утверждение $\sum_{i=1}^{m} \lambda_i \geq \sum_{i=1}^{m} \mu_i$ (то есть не для V, а для подпространства V, натянутого на первые m собственных векторов). Оно верно и без требования $q(x) \geq 0$. □

0.6. Метод главных компонент.

$a_0 = \frac{1}{s}\sum x_i$: $\langle u_1, \dots, u_k\rangle = L_0$, ортонорм, доп. до базиса, $\sum\limits_j ||pr_{L_0^\perp}(x_j - a)||^2 = \sum\limits_j (\sum\limits_{i=k+1}^{n} (x_{j,i} - a_i)^2)$, произв. L_0: S = $\sum\limits_{i=1}^{s} ||pr_{L_0}(x_i)||^2 \to max$; $X = (x_1, \dots, x_s)^T$. $S = \sum\limits_{i=1}^{k} q(u_i) = Tr\, q(x)|_{L_0}$, $q(u) = u^T X^T X u$. Макс. по КФ на $\langle v_1, \dots, v_k\rangle$

Пусть $V = \mathbb{R}^n$, $x_1, \dots, x_s \in V$.

Хочется найти афинное подпространство $L \le V$, $dim\, L = k$ такое, что сумма квадратов расстояний от x_i до L (вообще, корень из суммы квадратов, но на него забьём) минимальна.

Напоминание 1. $\rho(x, L) = ||pr_{L^\perp}(x)||$

Напоминание 2 (теорема Пифагора). $||pr_{L^\perp}(x)||^2 + ||pr_L(x)||^2 = ||x||^2$

Напоминание 3. $e_1, \dots, e_k$ — базис U (подпространства V). Тогда $pr_U(x) = \sum\limits_{i=1}^{k} \frac{\langle x, e_i\rangle}{\langle e_i, e_i\rangle} e_i$

Вывод алгоритма.

$L = L_0 + a$, где L_0 — линейное.

Сначала найдём a.

Теорема 7. Оптимально взять $a = \frac{1}{s}\sum\limits_{i=1}^{s} x_i$

Доказательство. Если из каждого x_i вычесть a, то все расстояния нужно будет считать до L_0.

$S = \sum\limits_{i=1}^{s} (\rho(x_i - a, L_0))^2 = \sum\limits_{i=1}^{s} ||pr_{L_0^\perp}(x_i - a)||^2$

Возьмём ортонормированный базис V u_i такой, что $u_1, \dots, u_k$ образуют базис L_0, а $u_{k+1}, \dots, u_n$ — дополнение до базиса.

$L_0^\perp = \langle u_{k+1}, \dots, u_n\rangle$.

$pr_{L_0^\perp}(x_j - a) = \sum\limits_{i=k+1}^{n} \frac{\langle x_j - a, u_i\rangle}{\langle u_i, u_i\rangle} u_i = \sum\limits_{i=k+1}^{n} \langle x_j - a, u_i\rangle u_i$ (так как u_i ортонормированны, $\langle u_i, u_i\rangle = 1$)

$||pr_{L_0^\perp}(x_j - a)||^2 = \langle \sum\limits_{i=k+1}^{n} \langle x_j - a, u_i\rangle u_i, \sum\limits_{i=k+1}^{n} \langle x_j - a, u_i\rangle u_i\rangle = \sum\limits_{i=k+1}^{n} \langle x_j - a, u_i\rangle^2$ (выживают только слагаемые с одинаковыми u_i, опять же, из-за ортонормированности)

$\langle x_j - a, u_i\rangle$ равняется i-ой координате $x_j - a$. А она, в свою очередь, равна $x_{j,i} - a_i$

$||pr_{L_0^\perp}(x_j - a)||^2 = \sum\limits_{i=k+1}^{n} (x_{j,i} - a_i)^2$

Мы минимизируем сумму квадратов расстояний по всем x. То есть:

$\sum\limits_{j=1}^{s} \sum\limits_{i=k+1}^{n} (x_{j,i} - a_i)^2$

Продифференцируем по a_i и найдём точку минимума:

$s \cdot 2a_i - 2\sum\limits_{j=1}^{s} x_{j,i} = 0$

$a_i = \frac{1}{s}\sum\limits_{j=1}^{s} x_{j,i}$

Проделав то же самое по всем i, получим $a = \frac{1}{s}\sum\limits_{j=1}^{s} x_j$. Это и хотели.

Поиск подходящего линейного подпространства L_0.

Мы хотим минимизировать сумму квадратов расстояний. Это (по теореме Пифагора (напоминание 2)) то же самое, что максимизировать сумму квадратов проекций на L (так как квадрат нормы x у нас фиксирован).

u_i — ортонормированный базис L_0.

$S = \sum\limits_{i=1}^{s} ||pr_{L_0}(x_i)||^2$

$pr_L(x_j) = \sum\limits_{i=1}^{k} \langle x_j, u_i\rangle u_i$ (по тем же соображениям, что и в прошлом пункте).

$S = \sum\limits_{i=1}^{s} \langle \sum\limits_{i=1}^{k} \langle x_j, u_i\rangle u_i, \sum\limits_{i=1}^{k} \langle x_j, u_i\rangle u_i\rangle = \sum\limits_{i=1}^{s} \sum\limits_{j=1}^{k} \langle x_i, u_j\rangle^2 = \sum\limits_{j=1}^{k} \sum\limits_{i=1}^{s} \langle x_i, u_j\rangle^2$ (u-шки ушли, так как базис ортонормированный).

Определим матрицу X следующим образом:

$$X = \begin{pmatrix} x_1^T \\ x_2^T \\ \vdots \\ x_s^T \end{pmatrix}$$

Это матрица размера $s \times n$
Посмотрим на результат $X \cdot u_j$:

$$A = \begin{pmatrix} \langle x_1, u_j \rangle \\ \vdots \\ \langle x_s, u_j \rangle \end{pmatrix}$$

Заметим, что если мы запишем $u_j^T \cdot X^T$, то получим A^T.
$A^T \cdot A = u_j^T X^T X u_j = \sum\limits_{i=1}^{s} \langle x_i, u_j \rangle^2$.
То есть, это значение квадратичной формы с матрицей $X^T X$ на векторе u_j.
$q(u) = u^T X^T X u$
Теперь $S = \sum\limits_{i=1}^{k} q(u_i) = Tr\, q(x)|_{L_0}$

По замечанию из неравенства на след (см. предыдущий билет) $S = Tr\, q(x)|_{L_0} \leq \sum\limits_{i=1}^{k} \lambda_i$. Но мы максимизируем S и знаем, на каком подпространстве достигается $\sum\limits_{i=1}^{k} \lambda_i$ (это подпространство $\langle v_1, \ldots, v_k \rangle$, где v_i — собственный вектор, соотвествующий собственному числу λ_i).

Таким образом, $L_0 = \langle v_1, \ldots, v_k \rangle$, где v_i — собственный вектор, соответствующий i-ому по убыванию собственному числу матрицы $X^T X$.

Алгоритм (обобщение).
Ищем афинное подпространство $L = L_0 + a$.
L_0 — линейное, $dim\, L_0 = k$
$a = \frac{1}{s} \sum\limits_{i=0}^{s} x_i$
Из каждого x_i вычли a.
Для новых векторов x построили матрицу

$$X = \begin{pmatrix} x_1^T \\ x_2^T \\ \vdots \\ x_s^T \end{pmatrix}$$

Нашли матрицу $C = X^T X$. Нашли её собственные числа $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ и собственные вектора $v_1, \ldots, v_n$, им соответствующие.
$L_0 = \langle v_1, \ldots, v_k \rangle$

0.7. Сингулярные значения и SVD-разложение.

Шпаргалка:
$X^* = X^\top, \langle X^* e_i, e_j \rangle = \langle e_i, X e_j \rangle, \sigma_i = \sqrt{d_i} > 0$ с.ч. $A^* A$. SVD $A\colon U \to V$ $\exists$ о/н $u_i, v_j\colon$ матр $A = \Sigma(\sigma_{1..r}$ на диаг) $(X = L\Sigma R)$. e_i – о/н с.в. $\langle Ae_i, Ae_j \rangle = \langle A^* A e_i, e_j \rangle = \langle d_i e_i, e_j \rangle, f_i = \frac{Ae_i}{\sqrt{d_i}}$ доп до базиса. $R = C^{-1} = C^\top, C$ столбцы e_i.

Напоминание Евклидово пространство – векторное пространство V над $\mathbb{R}$ вместе с заданной на нём билинейной симметричной формой $\langle \cdot, \cdot \rangle$.

Определение. Пусть A – линейное отображение $A\colon U \to V$ между евклидовыми пространствами. Тогда сопряжённым отображением к A называется такое линейное отображение $A^*\colon V \to U$, что $\langle A^* x, y \rangle = \langle x, Ay \rangle$ для всех $x \in V$ и $y \in U$.

Теорема 8. Сопряжённое линейное отображение единственно. Более того, если в U и V выбрать ортонормированные базисы, то матрица сопряжённого отображения в этих базисах будет равна транспонированной матрице исходного.

Доказательство. Достаточно доказать последнюю часть, чтобы показать единственность и существование. Выберем ортонормированные базисы в U и V – u_j и v_i. Обозначим матрицу A в этом базисе за X, а кандидата на A^* за X^*.

Для равенства из определения сопряжённости необходимо и достаточно его выполения на базисных векторах (так как скалярное произведение – билинейная функция). Иными словами необходимо и достаточно, чтобы выполнялось $\langle X^* e_i, e_j\rangle = \langle e_i, Xe_j\rangle$. Но первая часть даёт X^*_{ji}, а вторая – X_{ij}. Итого необходимо и достаточно, чтобы $X^* = X^\top$.

$$\langle X^* e_i, e_j\rangle = (X^* e_i)^\top e_j = \begin{pmatrix} X^*_{1i} \\ \vdots \\ X^*_{ni} \end{pmatrix}^\top e_j = X^*_{ji}$$

$$\langle e_i, Xe_j\rangle = e_i^\top X e_j = e_i^\top \begin{pmatrix} X_{1j} \\ \vdots \\ X_{mj} \end{pmatrix} = X_{ij}$$

□

Определение (Сингулярные значения)**.** Пусть A – линейное отображение $A\colon U \to V$ между евклидовыми пространствами. Тогда сингулярными значениями A называются числа $\sigma_i = \sqrt{d_i}$, где $d_i > 0$ – положительные собственные числа оператора $A^*A\colon U \to U$. Если же говорить на языке матриц, то для матрицы X её сингулярными значениями будут корни из собственных чисел $X^\top X$.

Singular Value Decomposition (сингулярное разложение) поясняет геометрический смысл сингулярных значений.

Теорема 9 (SVD разложение)**.** Пусть A – линейное отображение $A\colon U \to V$ между евклидовыми пространствами. Тогда существуют такие ортонормированные базисы U и V, что матрица A имеет вид

$$\Sigma = \begin{pmatrix} \sigma_1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \sigma_r & 0 \\ 0 & \dots & 0 & 0 \end{pmatrix},$$

где r – ранг A, числа $\sigma_1, \dots, \sigma_r$ его сингулярные значения. На языке матриц это означает, что для любой матрицы $X \in M_{m\times n}$ существуют матрицы L – размера m и R – размера n, что

$$X = L\Sigma R,$$

с теми же условиями на r и σ_i.

Доказательство. Рассмотрим оператор $B = A^*A$. Существует ортонормированный базис $e_1, \dots, e_n$, в котором оператор B диагонален, с неотрицательными числами на диагонали $d_1 \geq \dots \geq d_n \geq 0$.

[Почему такой базис существует: оператор самосопряженный, т. к. $(A^*A)^* = A^*A^{**} = A^*A$. В некотором ортонормированном базисе оператору соответствует неотрицательная матрица, значит, все собственные числа неотрицательные.]

Имеем $d_i = \sigma_i^2$ для единственного положительного σ_i. Посмотрим на вектора $Ae_i \in U$. Они ортогональны. Действительно

$$\langle Ae_i, Ae_j\rangle = \langle A^*Ae_i, e_j\rangle = \langle d_i e_i, e_j\rangle,$$

что равно нулю, если $i \neq j$. В случае $i = j$ получаем $||Ae_i||^2 = d_i$. Возьмём

$$f_i = \frac{Ae_i}{\sqrt{d_i}}$$

и дополним этот набор до ортонормированного базиса пространства V. Итого имеем $e_1, \dots, e_n$ ортонормированный базис U и $f_1, \dots, f_m$ – ортонормированный базис V. Посмотрим на матрицу A в этих базисах. По определению $Ae_i = \sqrt{d_i} f_i$. Это и даёт требуемый вид матрице оператора A

Поймем, как выглядит матрица R. В нашей конструкции матрица R есть матрица замены из стандартного базиса в базис из собственных векторов e_i матрицы $X^\top X$. Если за C обозначить матрицу из столбцов e_i (матрица замены из базиса из собственных векторов e_i в стандартный), то $R = C^{-1}$, но C ортогональна и поэтому можно написать $R = C^T$, то есть строки R – собственные вектора $X^\top X$. Часто эти вектора называют правыми сингулярными векторами X.

Матрица L – это матрица замены из базиса f_i в стандартный, то есть матрица из столбцов f_i.

□

Наличие такого разложения означает, что для всякого линейного отображения можно так выбрать декартову систему координат, что в этой системе координат это отображение будет выглядеть как растяжение вдоль каких-то осей.

0.8. Приближение матрицей указанного ранга и SVD-разложение...

Приближение матрицей указанного ранга и SVD-разложение. Возможность применения к сжатию изображения.

Шпаргалка:
pr из Б6 $\Leftrightarrow$ ближ по $||X||_F = \sqrt{\operatorname{Tr} X^\top X}$. $X = L\Sigma R$. pr на $\langle v_1^\top .. v_k^\top \rangle$. v_i базис $X^\top X$ и строки R. pr a на $V^{(k)} = \sum a v_i v_i^\top$. $X^{(k)} = L\Sigma(\sum R v_i v_i^\top) = L\Sigma R^{(k)} = L\Sigma^{(k)} R$. Сж $L^{(k)}\Sigma^{(k)}R^{(k)}$. $2kn + k \to 2kn$ при $k < \frac{n}{2}$. Минор $k^2 + 2k(n-k) + 2k$.

SVD-разложение используется в практическом решении задачи из метода главных компонент (билет 6) и позволяет сразу найти не только пространство, но и проекцию начальных точек на него. Формализуется это так: рассмотрим матрицу X, чьи строки равны $x_i^\top$. Тогда если все её строки заменить на их проекции на оптимальное подпространство L, то получится матрица ранга k или меньше (k – это размерность пространства, которое ищем). Эта матрица будет ближайшей к исходной в смысле вот такой вот матричной нормы, называемой, нормой Фробениуса

$$||X||_F = \sqrt{\sum_{i,j} a_{ij}^2} = \sqrt{\operatorname{Tr} X^\top X}.$$

Последнее равенство:

$$(X^\top X)_{jj} = \sum_i X_{ji}^\top X_{ij} = \sum_i X_{ij} X_{ij} = \sum_i a_{ij}^2$$

$$\operatorname{Tr} X^\top X = \sum_j (X^\top X)_{jj} = \sum_{i,j} a_{ij}^2$$

[Почему полученная матрица ближайшая к исходной: в 6 билете мы минимизировали $\sqrt{\sum ||x_i - pr_L x_i||^2} = \sqrt{\sum ||y_i||^2} = \sqrt{\sum y_{ij}^2}$. y_i – просто короткое обозначение для $x_i - pr_L x_i$.]

Таким образом нахождение проекций точек можно переформулировать как нахождение ближайшей к матрице X матрицы ранга меньше или равного k. Это легко сделать, зная SVD-разложение.

Теорема 10. Пусть $X \in M_{m\times n}(\mathbb{R})$. И SVD-разложение X имеет вид $X = L\Sigma R$, где на диагонали Σ стоят $\sigma_1, \ldots, \sigma_r$ и нули. Тогда наилучшим приближением ранга k в смысле нормы Фробениуса к матрице X будет матрица $X^{(k)} = L\Sigma^{(k)}R$, где на диагонали $\Sigma^{(k)}$ стоят $\sigma_1, \ldots, \sigma_k$ и нули.

Доказательство. Для того, чтобы найти матрицу $X^{(k)}$ необходимо спроецировать строки X на подпространство $L_k = \langle v_1^\top, \ldots, v_k^\top \rangle$, где v_i ортонормированный базис из собственных векторов $X^\top X$. Вспомним, что строки R есть $v_i^\top$.

Для того, чтобы спроецировать одну строку a на пространство $V^{(k)}$ необходимо вычислить сумму $\sum_{i=1}^k (av_i)v_i^\top$. $av_i = \langle a^\top, v_i \rangle$ – это как раз проекция a на v_i (коэффициент).

Применив это целиком к матрице $X = L\Sigma R$, получим

$$X^{(k)} = \sum_{i=1}^k X v_i v_i^\top = \sum_{i=1}^k L\Sigma R v_i v_i^\top = L\Sigma \left(\sum_{i=1}^k R v_i v_i^\top \right).$$

Вычислим последнюю сумму. Эта сумма считает проекции строк R на L_k. Но первые k строк лежат в L_k, а остальные ортогональны L_k. Итого имеем

$$R^{(k)} = \sum_{i=1}^k R v_i v_i^\top = \begin{pmatrix} v_1^\top \\ \vdots \\ v_k^\top \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Осталось заметить, что $\Sigma^{(k)}R = \Sigma^{(k)}R^{(k)} = \Sigma R^{(k)}$ (в произведении дальше k-ой строки или k-ого столбца в любом случае все 0). □

SVD-разложение используется в разных задачах, в том числе и для сжатия изображений. Для простоты рассмотрим случай квадратного $n\times n$ чёрно-белого изображения. Сделаем из него вещественную матрицу X размера $n\times n$ и найдём SVD-разложение $L\Sigma K$. Тогда приближение $X^{(k)}$ задаётся $L\Sigma^{(k)}R$. Однако, как мы уже заметили, вместо матрицы R можно взять матрицу $R^{(k)}$. Аналогично вместо L можно взять $L^{(k)}$ – выкинув из L последние $n-k$ столбцов. Для хранения матрицы $\Sigma^{(k)}$ нужно k параметров (она диагональная), для матриц $L^{(k)}$ и $R^{(k)}$ по kn параметров. Итого нужно $2kn + k$ параметров. Однако чтобы не хранить отдельно Σ её можно домножить на L и хранить $L\Sigma$. В таком случае необходимо $2kn$ параметров. При $k < \frac{n}{2}$ это даёт эффект сжатия.

Однако, это не предел. Посмотрим, сколько параметров нужно, чтобы задать X – матрицу ранга k. У нее есть невырожденная квадратная подматрица размера k. Пусть это просто первые k строк и столбцов. Тогда для j-ой строки матрицы, начиная с номера $j \geq k+1$ есть набор чисел $a_{1,j}, \ldots, a_{k,j}$, которые есть коэффициенты в линейной комбинации, дающей из первых k строк j-ую (набор из первых k строк и j-ой строки линейно зависим). Аналогично для столбцов. Такой набор данных задаётся $k^2 + 2k(n-k) = 2kn - k^2$ параметрами (k^2 коэффициентов квадратной подматрицы, по k коэффициентов линейной комбинации для $n-k$ строк и $n-k$ столбцов). Осталось заметить, что всегда $2kn - k^2 \leq n^2$ так как $0 \leq n^2 - 2kn + k^2 = (n-k)^2$. Если невырожденным оказался не главный минор, то дополнительно нужно задать $2k$ дискретных параметров, задающих номера строк и столбцов невырожденного минора.

0.9. Положительные матрицы. Теорема Перрона.

Шпаргалка: Док-во Перрона: положительность ($A|x| \geq |x| \Rightarrow A|x| < \frac{A^n}{(1+\varepsilon)^n} A|x| \to 0$ противореч.), единственность (сонапр. коорд. $v \Leftarrow \sum\limits_j A_{kj}|v_j| = |\sum\limits_j A_{kj}v_j|$) и некратность (Жорд. клетки; либо $\exists c, i : |x_1 - cx_2|_i = 0$, либо $Ax_2 = x_2 + x_1$)

Определение. Матрицу A назовем положительной, если все ее элементы строго положительны.

Определение. Матрицу A назовем неотрицательной, если все ее элементы неотрицательны.

Теорема 11 (Перрона)**.** Пусть матрица A положительна, λ ее наибольшее по модулю (!) собственное число. Тогда верны следующие утверждения:

1) Собственный вектор, соответствующий λ, положителен.
2) $\lambda > 0,\ \lambda \in \mathbb{R}$.
3) Модуль любого другого собственного числа строго меньше $|\lambda|$.
4) λ – не кратный корень характеристического многочлена A.

Доказательство. Пусть $|\lambda| = 1$ (иначе разделим все элементы матрицы на $|\lambda|$, это никак не повлияет на доказываемые утверждения). Обозначим за x собственный вектор с собственным числом λ.

1) Покажем, что $A|x| = |x|$ ($|x|$ – взять все координаты x по модулю). Это докажет первое утверждение. Для начала заметим, что
$$|x| = |Ax| \leq A|x|$$
Левое равенство следует из определения x, а правое неравенство нетрудно доказать, заметив, что при подсчете $A|x|$ мы работаем только с положительными числами. Однако вместо неравенства мы хотим получить равенство. Пусть все же $|x| < A|x|$. Обозначим $z = A|x|$. Тогда $y = z - |x| > 0$, а значит и $Ay > 0$. Выходит, что существует $\varepsilon > 0 : Ay > \varepsilon z$, следовательно $Ay = Az - A|x| = Az - z > \varepsilon z$ или же $\frac{A}{1+\varepsilon} z > z$. Из-за положительности z, A и ε, применяя оператор $\frac{A}{1+\varepsilon}$ к обеим частям неравенства, получим
$$\frac{A^n}{(1+\varepsilon)^n} z > \frac{A^{n-1}}{(1+\varepsilon)^{n-1}} z > \ldots > z$$
Но у оператора $\frac{A}{1+\epsilon}$ собственные числа меньше еденицы, поэтому $\lim\limits_{n\to\infty} \frac{A^n}{(1+\varepsilon)^n} z = 0$ (см. ниже). Получили противоречие с тем, что $z = A|x| > 0$.

Касательно факта про предел. Это следует из следствия 20 из конспекта прошлого семестра:

Пусть A – вещественная (или комплексная) матрица с собственным числом $\lambda_1 = 1$ кратности 1, а все остальные собственные числа A по модулю строго меньше 1. Если вектор $v = \sum c_i e_i$, где e_i жорданов базис, то
$$\lim_{n\to\infty} A^n v = c_1 e_1$$

2) Показав, что $A|x| = |x|$, мы попутно доказали $\lambda > 0,\ \lambda \in \mathbb{R}$
3) Рассмотрим собственное число μ ($|\mu| = 1$) с собственным вектором v. Тогда $A|v| = |v| = |Av|$. Поэтому все координаты $|Av|$ ненулевые (у $|v|$ есть хотя бы одна ненулевая координата $\Rightarrow$ у $A|v|$ все координаты ненулевые $\Rightarrow$ у $|Av|$ все координаты ненулевые). Распишем равенство $A|v| = |Av|$ для координаты k:
$$\sum_j A_{kj}|v_j| = v_k = |\sum_j A_{kj}v_j|$$

Посмотрим на это равенство, как на равенство норм векторов в $\mathbb{R}^2$ (v_j комплексные, поэтому можно представить, что это вектора над $\mathbb{R}^2$). Известно, что такое ненулевое равенство достигается только когда v_j сонаправлены. Значит любая их линейная комбинация (над $\mathbb{R}$) сонаправлена им, а поскольку координаты вектора Av как раз и есть линейные комбинации v_j, то выходит, что координаты Av и v отличаются друг от друга на вещественный множитель. $Av = \mu v \Rightarrow \mu \in \mathbb{R} \overset{A>0}{\Longrightarrow} \mu = 1$.

4) Пусть единица кратный корень. Тогда в Жордановой форме матрицы A либо найдутся хотя бы две Жордановы клетки с числом $\lambda = 1$ на диагонали, либо одна клетка размера хотя бы 2 (с λ на диагонали). Первому случаю соответствует наличие двух несонаправленных собственных векторов x_1 и x_2 с собственными числами, равными λ. Тогда подберём c, так что $v = x_1 - cx_2$ имеет нулевую координату. Получаем противоречие, так как $|x_1 - cx_2|$ – неотрицательный вектор с собственным числом 1, но при этом с нулевой координатой ($|v| = |Av| = A|v|$ и у $|v|$ есть хотя бы одна ненулевая координата $\Rightarrow$ у $A|v|$ все координаты ненулевые $\Rightarrow$ у v все координаты ненулевые).

   Во втором же случае x_2 присоединён к $x_1 > 0$, то есть $Ax_2 = x_2 + x_1$. Тогда имеем $A^n x_2 = x_2 + nx_1$. Это значит, что какие-то коэффициенты A^n растут по крайней мере линейно по n. Но тогда и коэффициенты $A^n x_1 = x_1$ тоже растут по крайней мере линейно, что очевидно не так.

□

0.10. Единственность положительного собственного вектора. Применение к случайному блужданию.

Шпаргалка: Знаем предел $\lim\limits_{k\to\infty} A^k v$, если у A макс по модулю с. ч. $\lambda = 1$ кратности 1. $A = P(G)$ нам не походит, замена $P(G)$: $P_\alpha(G) = (1-\alpha)P(G) + \alpha\frac{1}{n}J,\ \alpha \in (0,1),\ \forall i,j\ J_{ij} = 1$ – а это норм, Перрон гарантирует.

Лемма 6. Пусть $A > 0$, λ – максимальное по модулю собственное число. Если у матрицы A есть собственный вектор $y \geq 0$, то y – собственный вектор для числа λ

Доказательство. Рассмотрим матрицу $A^\top$. У неё есть положительный собственный вектор x, соответсвующий собственному числу λ. Пусть μ – собственное число для y. Тогда

$$\lambda x^\top y = x^\top A y = x^\top \mu y = \mu x^\top y.$$

Так как $x^\top y > 0$, то $\lambda = \mu$. □

Случайное блуждание

(Если я правильно понял идею, то все выглядит так:)

Пусть у нас есть набор страниц, каждая из которых ссылается на какие-то другие. Также есть пользователь, который произвольно их читает (случайно переходя по ссылкам). Обозначим за v – его исходное состояние (первую страницу, которую он читает). Хотим для каждой вершины узнать вероятность в ней оказаться после долгого блуждания по графу (вершины – страницы, ссылки – переходы). Это поможет нам отсортировать страницы по "полезности".

Определение. Матрица случайного блуждания $P(G)$:

$$P_{ij} = \begin{cases} \frac{1}{d_j}, \text{ если есть ребро } j \to i \\ 1, \text{ если из вершины не исходит рёбер} \\ 0, \text{ иначе} \end{cases}.$$

d_j – степень вершины j.

После одного перехода из v интересующие нас вероятности составляют вектор $P(G)v$. Значит нас интересует $\lim\limits_{n\to\infty} P(G)^n v$. Заметим, что для некоторого типа матриц такой предел известен (см. факт про предел $\to$ 1). Однако чтобы этим воспользоваться, нужно показать, что у $P(G)$ максимальное по модулю собственное число $\lambda = 1$, его кратность 1, а все остальные собственные числа A по модулю строго меньше 1. Воспользуемся теоремой Перрона.

Для начала заметим, что матрица $P(G)$ имеет довольно много нулевых компонент. И, строго говоря, теорема Перрона не может быть верна для $P(G)$ всегда. Как же она может помочь? Для этого мы схитрим и немного поменяем задачу. А именно, рассмотрим матрицу

$$P_\alpha(G) = (1-\alpha)P(G) + \alpha\frac{1}{n}J_n,$$

где J_n – матрица из одних единиц, а $\alpha \in (0,1)$. Тогда матрицы $P_\alpha(G)$ являются положительными. С точки зрения блуждающего пользователя это означает, что у него есть два режима – первый, в котором он находится с вероятностью $1-\alpha$ – это режим брождения по ссылкам (образующие граф G), а второй режим – переход на случайную страницу. Для

матрицы $P_\alpha(G)$ выполнены условия теоремы и поэтому она имеет единственное не кратное максимальное собственное число, которое положительно и соответствующий собственный вектор положителен. Покажем, что это собственное число равно 1.

Для этого рассмотрим матрицу $P_\alpha(G)^\top$. У этой матрицы есть положительный собственный вектор $(1,\dots,1)$ с собственным числом 1. Но тогда это максимальное по модулю собственное число для $P_\alpha(G)^\top$ и следовательно для $P_\alpha(G)$.

Теперь можем воспользоваться теоремой Перрона и найти предел $P_\alpha(G)^k v$, при $k\to\infty$. Он равен x – некоторому положительному вектору с собственным числом равным 1. Это позволяет приближённо найти x. Практически для этого можно взять $k\sim\log n$. Это позволяет заметно сэкономить на вычислениях по сравнению с теоретическим нахождением собственных векторов. Изучая предел $P_\alpha(G)$ при $\alpha\to 0$ можно получить информацию и про исходную матрицу.

0.11. Неориентированные графы. Собственные числа связного графа. Два примера.

Необработанная версия из конспекта Константина Михайловича

Определение. Спектр графа – это спектр его матрицы смежности $A(G)$.

Для начала разберёмся с оценками и свойствами собственных чисел матрицы смежности. Здесь нам пригодится теорема Перрона.

Лемма 7. Пусть граф G связен. Тогда его максимальное собственное число положительно, не кратно и соответствующий собственный вектор имеет положительные координаты. Более того, все собственные числа графа по модулю меньше чем максимальная степень d_{max}. Граф G регулярен тогда и только тогда, когда d_{max} – это его собственное число.

Доказательство. Прежде всего отметим, что все собственные числа G вещественные и максимальное собственное число положительно так как $\operatorname{Tr} A(G)=0$. Рассмотрим теперь матрицу $(A+\varepsilon I)^{n-1}$. Это положительная матрица. Действительно в $(A+\varepsilon I)^{n-1}_{ij}$ входит слагаемое ε^{n-1-l}, где l – длина пути между i и j. То же можно сказать и про большую степень $A+\varepsilon I$. Максимальное с.ч. A соответствует максимальному с.ч. $(A+\varepsilon I)^l$ по крайней мере, если ε очень большое. Но тогда соответствующий собственный вектор v положителен и максимальное собственное число $A+\varepsilon I$ и, следовательно, A не кратно. Далее v положительный собственный вектор для всех $(A+\varepsilon I)^l$, откуда получаем, что максимальное с.ч. у всех $(A+\varepsilon I)^l$ наибольшее по модулю $(\lambda_1+\varepsilon)^l > |\lambda_i+\varepsilon|^l$. Переходя к пределу при $\varepsilon\to 0$ получаем, что $\lambda_1^l\geq|\lambda_i|^l$. Осталось извлечь корень.

Почему же $\lambda_1\leq d_{max}$? Пусть x – собственный вектор для числа λ_1. Тогда $Ax=\lambda_1 x$. Посмотрим, насколько мог измениться x при домножении на A. Рассмотрим максимальную координату x_i. Имеем $\lambda_1 x_i=\sum a_{ij}x_j\leq d_{max}x_i$.

Предположим, что d_{max} собственное число. Тогда в указанном выше неравенстве достигается равенство, то есть $x_i=x_j$ для соседних вершин. Но это значит, что вектор $(1,\dots,1)$ собственный, что бывает только в случае регулярного графа. □

Примеры:
1) Спектр полного графа K_n равен $n-1$, $-1,\dots,-1$.
2) Спектр цикла длины n равен $2\cos(\frac{2\pi l}{n})$. Действительно, матрица смежности цикла имеет вид

$$C+C^{-1},\ \text{где } C=\begin{pmatrix}0 & & & 1\\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0\end{pmatrix}\ \text{матрица смежности ориентированного цикла.}$$

Так как собственные числа λ_l для C есть корни степени n из единицы, то

$$\lambda_l+\lambda_l^{-1}=\lambda_l+\overline{\lambda_l}=2\operatorname{Re}\lambda_l=2\cos\left(\frac{2\pi l}{n}\right)$$

0.12. Сильно регулярные графы. Граф Петерсона и его спектр. Двудольность и спектр.

$A^2+(\mu-\lambda)A+(\mu-k)E=\mu J$, $A^2_{|U}+(\mu-\lambda)A_{|U}+(\mu-k)E=0$ для $U=<(1,\cdots,1)>^\perp$
След степени == количество циклов == сумма собственных чисел с учетом кратности. λ для $(v,\ w)$, $-\lambda$ для $(v,\ -w)$

Определение. G - сильно регулярный $(n,\ k,\ \lambda,\ \mu)$, если это k-регулярный граф на n вершинах, причем у любых двух смежных вершин λ общих соседей, а у двух несмежных – μ общих соседей.

Теорема 12. Матрица сильно k-регулярного графа удовлетворяет соотношению $A^2 + (\mu - \lambda)A + (\mu - k)E = \mu J$, где J – это матрица из одних единиц.

Доказательство. Посмотрим на A^2. A^2_{ij} – число путей из i в j длины 2. Если i и j смежны, то $A^2_{ij} = \lambda$, если не смежны, то μ, если $i = j$, то k. Вычтем kE, получим нули на диагонали, вычтем λA, получим нули на позициях ребер, добавим $\mu A + \mu E$, чтобы заменить 0 на μ, получим μJ. □

Замечание. Если граф – сильно регулярный (для замечания, в общем случае верно и для регулярного), то у него есть собственный вектор $(1, \cdots, 1)$. Ограничим A на $U =< (1, \cdots, 1) >^{\perp}$. Тогда $A^2_{|U} + (\mu - \lambda)A_{|U} + (\mu - k)E = 0$. Поймем, почему справа 0. У оператора J_n ранка 1 есть n собственных чисел, одно из них – n с единственным собственным вектором $(1, \cdots, 1)$, остальные нули. При переходе к ортогональноу дополнению останутся только собственные числа 0, оператор, у которого все собственные числа 0 - нулевой.
здесь можно (и стоило бы) написать доказательство попроще, но я сходу не придумал

Следствие 1. Граф Петерсена сильно регулярен $(k = 3,\ \lambda = 0,\ \mu = 1)$, его спектр - $-2, -2, -2, -2, 1, 1, 1, 1, 1, 3$.

Доказательство. Подставим в полученное уравнение для ортогонального дополнения собственное число $A_{|U}$(если A удовлетворяет уравнению, то и его собственные числа тоже).
$x^2 + (1 - 0)x + (1 - 3) = 0,\ x^2 + x - 2 = 0$
$x_1 = -2,\ \ x_2 = 1$
Получим, что собственные числа - -2 и 1 с кратностями n_1 и n_2 соответственно. Тогда имеет место следующая система:

$$\begin{cases} n_1 + n_2 + 1 = 10, \\ -2n_1 + n_2 + 3 = \mathrm{Tr}(A) = 0. \end{cases}$$

Откуда $n_1 = 4$, $n_2 = 5$ (3 – наибольшее собственное число, 1 – его кратность) □

Теорема 13. Граф двудолен $\Leftrightarrow$ его спектр симметричен.

Доказательство. "$\Rightarrow$"
Пусть граф двудолен, тогда в каком-то базисе его матрицу смежности можно разбить на 4 подматрицы $A_{1,1} = 0$, $A_{1,2} = V$, $A_{2,1} = W$, $A_{2,2} = 0$ (нули - переходы из доли в себя же, V и W - переходы в соседнюю долю). Тогда несложно заметить $W = V^T$ (это никак не используется, просто прикольный факт).

$$\begin{pmatrix} 0 & V \\ W & 0 \end{pmatrix} \begin{pmatrix} v \\ w \end{pmatrix} = \begin{pmatrix} \lambda v \\ \lambda w \end{pmatrix} = \begin{pmatrix} Vw \\ Wv \end{pmatrix}, \ \begin{pmatrix} v \\ w \end{pmatrix} - \text{собственный вектор для } \lambda$$

Подставим вместо $\begin{pmatrix} v \\ w \end{pmatrix}$ $\begin{pmatrix} v \\ -w \end{pmatrix}$

$$\begin{pmatrix} 0 & V \\ W & 0 \end{pmatrix} \begin{pmatrix} v \\ -w \end{pmatrix} = \begin{pmatrix} V(-w) \\ Wv \end{pmatrix} = \begin{pmatrix} -Vw \\ Wv \end{pmatrix} = \begin{pmatrix} -\lambda v \\ -\lambda(-w) \end{pmatrix}$$

Т.е. мы получили, что $-\lambda$ также собственное число, т.е. спектр симметричен.
"$\Leftarrow$"
Граф двудолен $\Leftrightarrow$ нет нечетных циклов $\Leftrightarrow \mathrm{Tr}(A^k) = 0\ \forall k \equiv 1 (\mathrm{mod}\ 2)$
Но $\mathrm{Tr}(A^k)$ – сумма собственных чисел A^k, коими являются λ_i^k для собственных чисел λ_i A. Т.к. спектр симметричен, то $\lambda_i = -\lambda_j \Rightarrow \lambda_i^k = -\lambda_j^k$ для нечетного k, то есть след будет нулем (для каждого есть такой же с минусом). □

0.13. Две оценки на размер максимального независимого множества.

1. Натянуть подпространство на множество, следствие из Куранта-Фишера, нулевая квадратичная форма 2. Характеристический вектор множества, разложить по ортонорм. базису регулярного(!) графа с $u_1 = (1, \cdots, 1)\frac{1}{\sqrt{n}}$

Теорема 14. Пусть G - неориентированный граф на n вершинах, а A - симметричная матрица $n \times n$, такая, что если i не соединено с j, то $A_{ij} = 0$, то размер независимого множества не превышает $\min(n - n_+, n - n_-)$, где n_- - количество отрицательных собственных чисел A, а n_+ - положительных.

Доказательство. Рассмотрим подпространство, натянутое на вершины независимого множества (вектор, соответствующий вершине v_i - это нули на всех позициях, не равных i, и единица на позиции i). Тогда квадратичная форма $x^\top Ax$ при ограничении на это подпространство – нулевая. Это дает нам, что все собственные числа ограничения - нули. Если независимое множество имеет размер α, то и размер пространства, им порожденного - α. Получим α собственных чисел $\mu_1, \cdots, \mu_\alpha$. Но по следствию из теоремы Куранта-Фишера $\mu_1 \le \lambda_1$, $\mu_2 \le \lambda_2, \cdots, \mu_\alpha \le \lambda_\alpha$, при этом все $\mu_i = 0$, т.е. количество неотрицательных собственных чисел (а это как раз $n - n_-$) не меньше α. Аналогично можно доказать для неположительных (например, рассмотрев матрицу $-A$). □

Теорема 15. Пусть G - k-регулярный граф. Тогда размер его максимального независимого множества удовлетворяет неравенству

$$\alpha(G) \le -\frac{\lambda_n n}{k - \lambda_n}$$

Доказательство. Рассмотрим характеристичекий вектор v максимального независимого множества U ($v_i = 1$, если $i \in U$, 0 иначе).
Понятно, что $v^\top Av = 0$, $v^\top v = \alpha$. Т.к. граф регулярный, то есть нормированный собственный вектор $u_1 = \frac{1}{\sqrt{n}}(1, \cdots, 1)$. Тогда получим $\langle v, u_1\rangle = \frac{\alpha}{\sqrt{n}}$.
Разложим v по ортонормированной системе собственных векторов $u_1, \cdots, u_n$ $v = c_1u_1 + \cdots + c_nu_n$. Тогда

$$0 = v^\top Av = \sum c_i^2\lambda_i = c_1^2\lambda_1 + \sum_{i=2}^{n} c_i^2\lambda_i \ge c_1^2\lambda_1 + \lambda_n\sum_{i=2}^{n} c_i^2 = \lambda_1\frac{\alpha^2}{n} + \lambda_n\sum_{i=2}^{n} c_i^2$$

Известно $\sum c_i^2 = \alpha$ (как $\langle v, v\rangle$), тогда $\sum\limits_{i=2}^{n} c_i^2 = \alpha - \frac{\alpha^2}{n}$.
Получим

$$0 \ge \lambda_1\frac{\alpha^2}{n} + \lambda_n\left(\alpha - \frac{\alpha^2}{n}\right)$$

$$(\lambda_1 - \lambda_n)\frac{\alpha}{n} \le -\lambda_n$$

$$\alpha \le \frac{-\lambda_n n}{k - \lambda_n}$$

□

0.14. Три Петерсона

K_{10} не покрывается тремя Петерсонами.

$\sum\limits_{i=1}^{3} A_i = B$. Все рег $\Rightarrow$ общий с.в. $(1, \ldots, 1)$ для P с.ч. 3, для полного с.ч. 9. Сузим. Для A_1 и A_2 подпр. порожд. с.в. с с.ч. 1 $\cap$. Распишем для u из $\cap$. $Bu = -u$ (натянуто на с.в. с с.ч. -1). $\Rightarrow$ с.в. для A_3 с с.ч. -3. Такого с.ч. нет.

Пусть есть граф K_{10} (полный граф на 10 вершинах). В нём 45 рёбер. А ещё у нас есть граф Петерсона. В нём 15 рёбер. Хочется покрыть K_{10} тремя Петерсонами. Но это невозможно, потому что:

Теорема 16. K_{10} не представим в виде дизъюнктного объединения $P_1 \sqcup P_2 \sqcup P_3$, где P_1, P_2, P_3 — графы Петерсона.

Доказательство. Посмотрим на равенство $K_{10} = P_1 \sqcup P_2 \sqcup P_3$ в матричном виде.

Это означает, что $A_1 + A_2 + A_3 = B$, где A_1, A_2, A_3 — матрицы Петерсонов, B — матрица полного.

Но мы знаем для них собственные числа. Для Петерсона это $\{3, 1, 1, 1, 1, 1, -2, -2, -2, -2\}$, для $B = J_n - E$ (J_n — матрица из одних единиц) — это $\{n - 1 = 9, -1$ кратности $9\}$

Более того, все графы в нашем равенстве регулярные $\Rightarrow^{\text{(по лемме из какого-то прошлого билета)}}$ $v = (1, \ldots, 1)^T$ — собственный вектор для каждого из них. Для Петерсонов у него собственное число 3, а для полного $n - 1 = 9$.

Тогда перейдём на подпространство $U = \langle v\rangle^\perp$. Его размерность 9.

Рассмотрим A_1 и A_2. В них есть подпространства U_1, U_2 размерности 5, порождённые собственными векторами с собственным числом 1 $\Rightarrow$ эти пространства пересекаются $\Rightarrow \exists\ u \in U_1 \cap U_2$.

$A_1 + A_2 = B - A_3$.

$A_1u + A_2u = Bu - A_3u$.

Знаем, что $A_1u = A_2u = u$. Так же знаем, что $Bu = -u$, так как ортогональное дополнение натянуто на подпространство из векторов с собственным числом -1.

$\Rightarrow$ $A_3u = -u - u - u = -3u$. Получается, что u — собственный вектор A_3 с собственным числом -3. Но у A_3 нет такого собственного числа. Противоречие. □

0.15. Тензорное произведение. Существование.

Шпаргалка: TODO

Определение. Пусть есть набор пространств $V_1, \dots, V_n$. Тогда их тензорным произведением называется пространство $V_1 \otimes \dots \otimes V_n$ вместе с полилинейным отображением

$$i \colon V_1 \times \dots \times V_n \to V_1 \otimes \dots \otimes V_n,$$

удовлетворяющее условию: для любого полилинейного отображения $h \colon V_1 \times \dots \times V_n \to U$ существует единственное линейное отображение

$$\hat{h} \colon V_1 \otimes \dots \otimes V_n \to U,$$

что

$$\hat{h} \circ i = h.$$

Иными словами, отображение i – это «универсальное» полилинейное отображение.

Теорема 17. Пусть $V_1, \dots, V_n$ – набор векторных пространств над полем K. Тогда имеет место следующая конструкция тензорного произведения:

$$V_1 \otimes \dots \otimes V_n \cong K\langle V_1 \times \dots \times V_n \rangle / Rel,$$

где Rel – это подпространство, порождённое формальными суммами

$$(\dots, \lambda v + u, \dots) - \lambda(\dots, v, \dots) - (\dots, u, \dots).$$

Доказательство. Для удобства обозначим пространство

$$T = K\langle V_1 \times \dots \times V_n \rangle / Rel.$$

[$K\langle V_1 \times \dots \times V_n \rangle$ – пространство, натянутое на множество $V_1 \times \dots \times V_n$, т. е. пространство всех формальных сумм $\sum \lambda_i (v_{1_i}, \dots, v_{k_i})$]

Будем обозначать образы элементов $(v_1, \dots, v_n)$ в T как $v_1 \otimes \dots \otimes v_n$. Отображение

$$i \colon V_1 \times \dots \times V_n \to T$$

отображающее

$$(v_1, \dots, v_n) \to v_1 \otimes \dots \otimes v_n$$

полилинейно по самому определению соотношений из Rel. Действительно, для полилинейности нужно, чтобы

$$v_1 \otimes \dots \otimes (\lambda v_i + u_i) \otimes \dots \otimes v_n = \lambda v_1 \otimes \dots \otimes v_i \otimes \dots \otimes v_n + v_1 \otimes \dots \otimes u_i \otimes \dots \otimes v_n$$

Это эквивалентно тому, что все формальные суммы из Rel в T должны быть 0.

Пусть теперь дано пространство U и полилинейное отображение

$$h \colon V_1 \times \dots \times V_n \to U.$$

Построим отображение $\hat{h}$ следующим образом: сначала определим $\hat{\hat{h}} \colon K\langle V_1 \times \dots \times V_n \rangle \to U$, а затем покажем, что оно пропускается через T. По самому своему определению $K\langle V_1 \times \dots \times V_n \rangle$ имеет базисом элементы $(v_1, \dots, v_n)$. Отображение $\hat{\hat{h}}$ достаточно задать на них. Положим

$$\hat{\hat{h}}((v_1, \dots, v_n)) = h(v_1, \dots, v_n).$$

Покажем, что оно однозначно пропускается через T. Единственность очевидна (заданы образы всех базисных). Для того чтобы показать, что $\hat{\hat{h}}$ пропускается через T необходимо показать, что все соотношения лежат в ядре $\hat{\hat{h}}$.

$$\hat{\hat{h}}((\dots, \lambda v_i + u_i, \dots) - \lambda(\dots, v_i, \dots) - (\dots, u_i, \dots)) = h(\dots, \lambda v_i + u_i, \dots) - \lambda h(\dots, v_i, \dots) - h(\dots, u_i, \dots) =$$

$$\lambda h(\dots, v_i, \dots) + (\dots, u_i, \dots) - \lambda(\dots, v_i, \dots) - (\dots, u_i, \dots) = 0$$

□

Определение. Будем обозначать элемент $i(v_1, \dots, v_n) = v_1 \otimes \dots \otimes v_n$.

0.16. Единственность тензорного произведения. Размерность тензорного произведения.

Шпаргалка: TODO

Теорема 18. Тензорное произведение единственно с точностью до изоморфизма.

Доказательство. Допустим, есть два тензорных произведения $(V_1 \otimes \dots V_n)_1$ и $(V_1 \otimes \dots V_n)_2$ и их полилинейные отображения i_1 и i_2. Тогда по определению существуют единственные линейные отображения $\hat{i}_1$ и $\hat{i}_2$, что

$$\hat{i}_1 \colon (V_1 \otimes \dots V_n)_2 \to (V_1 \otimes \dots V_n)_1,\ \hat{i}_1 \circ i_2 = i_1$$

$$\hat{i}_2 \colon (V_1 \otimes \dots V_n)_1 \to (V_1 \otimes \dots V_n)_2,\ \hat{i}_2 \circ i_1 = i_2$$

Нужно проверить, что $\hat{i}_1$ и $\hat{i}_2$ взаимно обратны. Проверим, что $\hat{i}_1 \circ \hat{i}_2 \circ i_1 = i_1$ и $\hat{i}_2 \circ \hat{i}_1 \circ i_2 = i_2$. Это будет значить, что $\hat{i}_1 \hat{i}_2 = \mathrm{Id}$.

$$\hat{i}_1 \circ (\hat{i}_2 \circ i_1) = \hat{i}_1 \circ i_2 = i_1$$
$$\hat{i}_2 \circ (\hat{i}_1 \circ i_2) = \hat{i}_2 \circ i_1 = i_2$$

□

Теорема 19. Пусть $e_{i1}, \dots, e_{ik}$ базис V_i. Тогда $e_{1j_1} \otimes \dots \otimes e_{nj_n}$ базис $V_1 \otimes \dots \otimes V_n$. В частности,

$$\dim V_1 \otimes \dots \otimes V_n = \prod_{i=1}^{n} \dim V_i.$$

Доказательство. Прежде всего заметим, что набор $e_{1j_1} \otimes \dots \otimes e_{nj_n}$ является порождающей системой для тензорного произведения. $v_1 \otimes \dots \otimes v_n = (\sum\limits_j c_j e_{1j}) \otimes v_2 \otimes \dots \otimes v_n = \sum\limits_j c_j e_{1j} \otimes v_2 \otimes \dots \otimes v_n$. И вот так же можно раскрыть все по полилинейности, чтобы остались только $e_{1j_1} \otimes \dots \otimes e_{nj_n}$.

Далее, по определению тензорного произведения,

$$\mathrm{Hom}(V_1, \dots, V_n, K) \cong \mathrm{Hom}(V_1 \otimes \dots \otimes V_n, K).$$

Размерность последнего пространства совпадает с размерностью $V_1 \otimes \dots \otimes V_n$ (это двойственное пространство). С другой стороны, полилинейное отображение $h \in \mathrm{Hom}(V_1, \dots, V_n, K)$ однозначно задаётся $\prod_{i=1}^{n} \dim V_i$ параметрами $h(e_{1j_1}, \dots, e_{nj_n})$. Комбинируя эти два факта получаем, что размерность $\dim V_1 \otimes \dots \otimes V_n$ есть $\prod_{i=1}^{n} \dim V_i$. Отсюда, любая порождающая система такого размера есть базис. В частности, набор $e_{1j_1} \otimes \dots \otimes e_{nj_n}$. □

0.17. Тензорное произведение...

Тензорное произведение линейных отображений. Кронекерово произведение. Тензорное произведение операторов и его собственные числа. Категорное произведение графов.

Единств: определено на тензорятах; $\exists$: отобразить $U_1 \times \dots \times U_k$ в $V_1 \otimes \dots \otimes V_K$ полилин. (композ полилин.) $\Rightarrow$ (опр. тенз.) $\exists!$. Наше правило подходит. Матрица: расписать $(\sum\limits_k A_{k,i} f_k) \otimes (\sum\limits_l B_{l,j} f'_l)$. С.ч. $A \otimes B$: жорданов базис.

Определение. Тензорное произведение линейных отображений.

Пусть есть набор линейных отображений $f_i :\ U_i \to V_i$. Определим отображение

$$f_1 \otimes \dots \otimes f_n :\ \otimes U_i \to \otimes V_i$$

по правилу

$$(f_1 \otimes \dots \otimes f_n)(u_1 \otimes \dots \otimes u_n) = f_1(u_1) \otimes \dots \otimes f_n(u_n).$$

Лемма 8. Отображение с таким свойством единственно.

Доказательство. Таким отображением мы определили значения $(f_1 \otimes \dots \otimes f_n)$ на базисе $(\otimes U_i)$, так как базис состоит из какого-то подмножества тензорят, а отображение мы определили от каждого тензорёнка. □

Лемма 9. Указанное отображение корректно задано.

Доказательство. Рассмотрим диаграмму:

$$\begin{array}{ccc} U_1 \times \cdots \times U_k & \xrightarrow{(f_1, \cdots, f_k)} & V_1 \times \cdots \times V_k \\ \downarrow & & \downarrow T \\ U_1 \otimes \cdots \otimes U_k & \xrightarrow[f_1 \otimes \cdots \otimes f_n(?)]{} & V_1 \otimes \cdots \otimes V_k \end{array}$$

Посмотрим на композицию $T \circ (f_1, \cdots, f_k)$. Она полилинейна, так как это композиция двух полилинейных отображений.

Значит (по определению тензорного произведения) существует и единственно линейное отображение $f_1 \otimes \cdots \otimes f_n$.

Заметим, что это отображение удовлетворяет нашему требованию $(f_1 \otimes \cdots \otimes f_k)(u_1 \otimes \cdots \otimes u_k) = f_1(u_1) \otimes \cdots \otimes f_k(u_k)$, так как для набора $(u_1, \cdots, u_k)$: $(f_1 \otimes \cdots \otimes f_k)(u_1 \otimes \cdots \otimes u_k) = T(f_1(u_1), \cdots f_k(u_k)) = f_1(u_1) \otimes \cdots \otimes f_k(u_k)$ □

Теперь хочется разобраться с тем, как выглядит матрица тензорного произведения линейных отображений.

Лемма 10. Пусть $L_1 \colon V_1 \to U_1$, а $L_2 \colon V_2 \to U_2$. Пусть $e_1, \ldots, e_{n_1}$ базис V_1, $e'_1, \ldots, e'_{n_2}$ базис V_2, и $f_1, \ldots, f_{m_1}$ – базис U_1, а $f'_1, \ldots, f'_{m_2}$ – базис U_2. Упорядочим базисы тензорных произведений – удобно это сделать, например, в лексикографическом порядке (номер первой координаты важнее). Тогда матрица $L_1 \otimes L_2$ разобьётся на $n_1 m_1$ блоков в каждом из которых будет стоять $A_{ij}B$, где i, j – номер блока, а A и B матрицы L_1 и L_2 соответственно.

Доказательство. По определению тензорного произведения отображений: $(L_1 \otimes L_2)(e_i \otimes e'_j) = L_1(e_i) \otimes L_2(e'_j) = (Ae_i) \otimes (Be'_j) = (\sum\limits_k A_{k,i} f_k) \otimes (\sum\limits_l B_{l,j} f'_l)$

Когда раскроем скобки, при $f_k \otimes f'_l$ будет коэффицент $A_{k,i} \cdot B_{l,j}$

Получился столбец матрицы:

$$\begin{pmatrix} A_{1,i} \cdot B_{1,j} \\ A_{1,i} \cdot B_{2,j} \\ \vdots \\ A_{1,i} \cdot B_{m_2,j} \\ \vdots \\ A_{m_1,i} \cdot B_{m_2,j} \end{pmatrix}$$

Это столбец при $e_i \otimes e'_j$ той матрицы, что и хотели. □

Определение. Такая матрица называется **кронекеровым (или тензорным) произведением** матриц A и B и обозначается $A \otimes B$.

Лемма 11. У оператора $A \otimes B$ собственные числа — это попарные произведения с.ч. для A и B.

Доказательство. Действительно, рассмотрим жорданов базис для A и B — $v_1, \ldots, v_n$ и $u_1, \ldots, u_m$. Тогда рассмотрев базис $v_i \otimes u_j$ заметим, что под диагональю будут стоять нули, а на диагонали — попарные произведения собственных чисел A и B. □

Определение. Пусть G и H — два графа (возможно, ориентированных). Тогда их **категорным произведением** называется граф чьи вершины есть пары вершин G и H и ребро между парами (u_1, v_1) и (u_2, v_2) проводится только если есть рёбра $u_1 \to u_2$ и $v_1 \to v_2$. **Декартовым произведением** графов G и H называется граф на тех же вершинах с ребром между парами если $u_1 = u_2$ и есть ребро $v_1 \to v_2$ или, симметрично, $v_1 = v_2$ и есть ребро $u_1 \to u_2$. Разумеется для неориентированных графов эта конструкция снова выдаёт неориентированный граф.

Обозначается $G \times H$

Лемма 12. Спектр категорного произведения графов состоит из всех возможных попарных произведений собственных чисел графов.

Доказательство. Заметим, что матрица смежности категорного произведения графов — это тензорное произведение матриц смежности исходных графов.

Более формально: $A(G_1 \times G_2) = A(G_1 \otimes G_2)$. Во втором случае единички стоят только там, где есть оба ребра. Этого и хотели. □

0.18. Канонические изоморфизмы для тензорного произведения.

3. $\mathrm{Hom}(U,V) \cong V \otimes U^*$: $v \times f \to (u \to f(u)v)$. 4. $\mathrm{Hom}(U \otimes V, W) \cong \mathrm{Hom}(U, \mathrm{Hom}(V,W))$: $L_1 :\ L \to (u \to (v \to L(u \otimes v)))$, $L_2 :\ L \to (u \otimes v \to (L(u))(v))$, они обратны. 5. $U^* \otimes V^* \to (U \otimes V)^*$: $f \otimes g \to (u \otimes v \to f(u)g(v))$ базис в базис

С понятием тензорного произведения связан ряд канонических отождествлений между разными на первый взгляд пространствами в духе изоморфизма $V \sim V^{**}$.

Теорема 20. Имеют место следующие естественные изоморфизмы:

$$(U \otimes V) \otimes W \cong U \otimes V \otimes W \cong U \otimes (V \otimes W)$$

$$U \otimes V \cong V \otimes U$$

$$\mathrm{Hom}(U,V) \cong V \otimes U^*$$

$$\mathrm{Hom}(U \otimes V, W) \cong \mathrm{Hom}(U, \mathrm{Hom}(V,W))$$

$$(U \otimes V)^* \cong U^* \otimes V^*$$

Доказательство. Наиболее интересная часть этой теоремы состоит в бескоординатном построении этих отображений.

Первое. Докажем только первую часть, остальное аналогично.

$$\begin{array}{ccc} U \times V \times W & \xrightarrow{\quad A \quad} & (U \otimes V) \times W \\ {\scriptstyle B}\downarrow & & \downarrow{\scriptstyle C} \\ U \otimes V \otimes W & \xrightarrow[\quad D \quad]{} & (U \otimes V) \otimes W \end{array}$$

$C \circ A$ полилинейно $\Rightarrow \exists!$ D линейное. D, заданное по правилу $u \otimes v \otimes w \to (u \otimes v) \otimes w$ подходит (если не верите, пропустите (u,v,w) через $C \circ A$ и через B).

Это изоморфизм, потому что базис переводит в базис (а можно по-честному найти обратную стрелку и сказать, что их композиция тождественна).

Второй пункт считаю очевидным (там надо отобразиться из $V \times U$ в $U \times V$ и радоваться жизни).

Третий. Построим отображение $V \times U^* \to Hom(U,V)$ по правилу

$$v \times f \to (u \to f(u)v).$$

Это соответствие полилинейно по v, f поэтому есть диаграмма:

$$\begin{array}{ccc} U^* \times V & \xrightarrow{(f,v) \to (u \to f(u)v)} & Hom(U,V) \\ {\scriptstyle B}\downarrow & \overset{A}{\nearrow} & \\ U^* \otimes V & & \end{array}$$

A линейное существует и единственно. $A :\ (f \otimes v) \to (u \to f(u)v)$ подходит.

Для изоморфизма осталось проверить, что базис переводит в базис. Пусть e_i базис V, f_j – базис U, а f^j базис U^*. Тогда $f^j \otimes e_i$ соответствует линейное отображение с матрицей

$$e_{ij} = \begin{array}{c} \\ i \end{array} \begin{array}{c} \begin{array}{cccc} & & j & \end{array} \\ \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & \ddots & & \vdots \\ \vdots & 1 & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix} \end{array}$$

Такие линейные отображения образуют базис $\mathrm{Hom}(U,V)$.

Четвёртое. Рассмотрим отображение $\mathrm{Hom}(U \otimes V, W) \to \mathrm{Hom}(U, \mathrm{Hom}(V,W))$ заданное по правилу

$$L_1 :\ L \to (u \to (v \to L(u \otimes v))).$$

Правая часть линейна и по u и по v, что значит, что это действительно отображение в $\mathrm{Hom}(U, \mathrm{Hom}(V,W))$. Теперь построим обратное отображение:

$$L_2 :\ L \to (u \otimes v \to (L(u))(v))$$

Внутреннее отображение полилинейно по u, v и поэтому дает корректное отображение из тензорного произведения в W. Они взаимно обратны:

WARNING! Скорее всего есть доказательство лучше и короче, но я не очень умный.

$$Y : u \otimes v \to w_{uv}$$

$$L_1(Y) = u \to (v \to w_{uv})$$

$$((L_1(Y))(u) = v \to w_{uv}$$

$$(((L_1(Y))(u))(v) = w_{uv}$$

$$L_2(L_1(Y)) = u \otimes v \to w_{uv} = Y$$

Что и хотели.
Пятое. Построим отображение $U^* \otimes V^* \to (U \otimes V)^*$. Зададим его правилом

$$f \otimes g \to (u \otimes v \to f(u)g(v))$$

Отображение справа полилинейно по u, v и даёт корректное отображение из тензорного произведения. Теперь вся правая часть полилинейна по f, g, и поэтому всё отображение задано. Если u_i базис U и v_j базис V, то тензорёнок $u^i \otimes v^j$ переходит в элемент двойственного базиса к $\{u_i \otimes v_j\}$. Это показывает, что данное отображение есть изоморфизм. □

0.19. Тензоры. Примеры. Координаты тензора. Замена переменной – случай тензора валентности (1,0).

Необработанная версия из конспекта Константина Михайловича

Дадим определение:

Определение. Тензором валентности (p, q) на пространстве V называется элемент пространства $V^{*\otimes p} \otimes V^{\otimes q}$. Так же будем говорить, что такие элементы – это p раз ковариантные и q раз контравариантные тензоры. Тензорами валентности $(0, 0)$ называются элементы поля K – скаляры.

Теперь я утверждаю, что более менее все встречавшиеся нам структуры на векторном пространстве V являются тензорами.

Примеры:

1) Вектор $v \in V$ является 1 раз контравариантным тензором.
2) Элемент двойственного пространства $f \in V^*$ является 1 раз ковариантным тензором. Вообще ковариантными называют тензоры, которые соответствуют полилинейным формам на пространстве V. Это историческая традиция. Точнее:
3) Так как пространство $V^{*\otimes p} \cong (V^{\otimes p})^* \cong \mathrm{Hom}(V, \dots, V, K)$, то тензор валентности $(p, 0)$ соответствует полилинейному отображению $V \times \dots \times V \to K$.
4) В частности, тензор валентности $(2, 0)$ – это билинейная форма.
5) Линейный оператор – это элемент $\mathrm{Hom}(V, V) \cong V^* \otimes V$, то есть тензор валентности $(1, 1)$.
6) Структура алгебры на V (без требования ассоциативности) задаётся билинейным отображением $V \times V \to V$, то есть линейным отображением $V \otimes V \to V$ или же элементом $V^* \otimes V^* \otimes V$, то есть тензором типа $(2, 1)$.

Как записать тензор в координатах? Выберем базис $e_1, \dots, e_n$ пространства V и возьмём в двойственном пространстве двойственный базис $e^1, \dots, e^n$. Теперь построим базис тензорного произведения $V^{*\otimes p} \otimes V^{\otimes q}$. Он имеет вид $e^{j_1} \otimes \dots \otimes e^{j_p} \otimes e_{i_1} \otimes \dots \otimes e_{i_q}$. Тогда произвольный тензор T валентности (p, q) имеет вид

$$T = \sum_{\substack{i_1,\dots,i_q \in \overline{1,n} \\ j_1,\dots,j_p \in \overline{1,n}}} T^{i_1,\dots,i_q}_{j_1,\dots,j_p} \, e^{j_1} \otimes \dots \otimes e^{j_p} \otimes e_{i_1} \otimes \dots \otimes e_{i_q}.$$

Элементы $T^{i_1,\dots,i_q}_{j_1,\dots,j_p}$ называются координатами тензора T.

Как меняются координаты тензора при замене базиса? Посмотрим сначала на случай тензоров типа $(1, 0)$.

Теорема 21. Пусть $e_1, \dots, e_n$ старый базис V, а $\hat{e}_1, \dots, \hat{e}_n$ – новый. Пусть C – матрица перехода из старого базиса в новый. Тогда матрица перехода из базиса $e^1, \dots, e^n$ в базис $\hat{e}^1, \dots, \hat{e}^n$ есть $C^{\top -1}$.

Доказательство. Зафиксируем конвенцию: матрица C это такая матрица, что для всякого вектора v со старыми координатами x и новыми координатами y выполнено, что $y = Cx$. В частности, это выполнено для вектора e_i. Это означает, что вектор $e_i = \sum_{j=1}^{n} C_{ji}\hat{e}_j$. Собственно, это ещё одна характеризация матрицы C. Наша задача найти матрицу D, со свойством $e^i = \sum D_{ji}\hat{e}^j$. По определению $e^k(e_i) = \delta_{ki}$. Подставим вместо e^k и e_i выражения с матрицами C и D. Имеем

$$\delta_{ki} = \sum_j C_{ji} \sum_l D_{lk}\hat{e}^l(\hat{e}_j) = \sum_{j,l} C_{ji}D_{lk} \cdot \delta_{lj} = \sum_j C_{ji}D_{jk}$$

Теперь это равенство можно проинтерпретировать при помощи матричного произведения как

$$E_n = C^\top D,$$

что и доказывает требуемое. □

0.20. Замена переменной – общий случай.

Необработанная версия из конспекта Константина Михайловича

Теперь мы можем разобраться с тензорами общего вида:

Теорема 22. Пусть $e_1, \ldots, e_n$ старый базис V, а $\hat{e}_1, \ldots, \hat{e}_n$ – новый. Пусть C – матрица перехода из старого базиса в новый, а $D = {C^\top}^{-1}$. Тогда координаты тензора T в базисе $\hat{e}$ выражаются через старые координаты следующим образом:

$$\hat{T}^{i_1,\ldots,i_q}_{j_1,\ldots,j_p} = \sum_{\substack{i'_1,\ldots,i'_q \in \overline{1,n} \\ j'_1,\ldots,j'_p \in \overline{1,n}}} \prod_{t \in \overline{1,p}} D_{j_t,j'_t} \prod_{s \in \overline{1,q}} C_{i_s,i'_s}\, T^{i'_1,\ldots,i'_q}_{j'_1,\ldots,j'_p}.$$

Доказательство. Обозначим за $e^{j_1,\ldots,j_p}_{i_1,\ldots,i_q}$ тензор $e^{j_1} \otimes \cdots \otimes e^{j_p} \otimes e_{i_1} \otimes \cdots \otimes e_{i_q}$. Рассмотрим тензор

$$T = \sum_{\substack{i'_1,\ldots,i'_q \in \overline{1,n} \\ j'_1,\ldots,j'_p \in \overline{1,n}}} T^{i'_1,\ldots,i'_q}_{j'_1,\ldots,j'_p} e^{j'_1,\ldots,j'_p}_{i'_1,\ldots,i'_q}$$

и заменим $e_i = \sum_{j=1}^{n} C_{ji}\hat{e}_j$ и $e^i = \sum D_{ji}\hat{e}^j$. Получится такая сумма:

$$T = \sum_{\substack{i'_1,\ldots,i'_q \in \overline{1,n} \\ j'_1,\ldots,j'_p \in \overline{1,n}}} T^{i'_1,\ldots,i'_q}_{j'_1,\ldots,j'_p} \sum_{\substack{i_1,\ldots,i_q \in \overline{1,n} \\ j_1,\ldots,j_p \in \overline{1,n}}} D_{j_1j'_1} \ldots D_{j_pj'_p} C_{i_1i'_1} \ldots C_{i_qi'_q} \hat{e}^{j_1,\ldots,j_p}_{i_1,\ldots,i_q}$$

Осталось поменять суммирование местами. □

Важность тензоров в теоретической физике обуславливается тем, что практически все физические объекты – это тензоры. Точнее: с точки зрения теории относительности пространство-время это некоторое четырёхмерное многообразие M (в двумерной ситуации подошла бы обычная сфера или тор). С каждой точкой x этого многообразия связано касательное пространство в этой точке – некоторое четырёхмерное пространство T_x. Представим себе, что в каждой точке пространства задана плотность вещества (на самом деле не так, но допустим) – это даёт вам функцию $f\colon M \to \mathbb{R}$ – скаляр в каждой точке, то есть тензор типа $(0,0)$.

Направление движения материи можно задать взяв в каждой точке касательный вектор, то есть тензор ранга $(0,1)$ на T_x. Дальше, у каждого такого вектора можно считать его «длину» и углы между векторами. Для этого надо задать для каждой точки x билинейную форму на касательном пространстве, то есть элемент $T^{(2,0)}_x$. И т.д. Чаще всего такие объекты называют тензорными полями, если хочется подчеркнуть, что в разных точках это тензор вообще говоря на разных пространствах.

Важно, что уравнения в физике не должны зависеть от выбора координат. Можно, конечно, писать какие-то уравнения при помощи координат тензоров и каждый раз проверять, что выбрав новые координаты уравнение будет того же вида. Однако, чем сложнее наука тем сложнее становятся проверки. Становится важно работать с тензорами не рассматривая их координаты. Для этого мы обсудим две операции с тензорами, которые легко можно понять не используя координаты. Начнём с самой простой – умножение тензоров.

0.21. Тензорная алгебра. Свёртка и след.

Необработанная версия из конспекта Константина Михайловича

Определение. Рассмотрим пространства $V^{p,q}$ и $V^{p',q'}$. Тогда имеет место билинейное отображение

$$V^{p,q} \times V^{p',q'} \to V^{p+p',q+q'},$$

заданное правилом

$$(v^1 \otimes \cdots \otimes v^p \otimes u_1 \otimes \cdots \otimes u_q, \hat{v}^1 \otimes \cdots \otimes \hat{v}^{p'} \otimes \hat{u}_1 \otimes \cdots \otimes \hat{u}_{q'}) \to v^1 \otimes \cdots \otimes v^p \otimes \hat{v}^1 \otimes \cdots \otimes \hat{v}^{p'} \otimes u_1 \otimes \cdots \otimes u_q \otimes \hat{u}_1 \otimes \cdots \otimes \hat{u}_{q'}.$$

Такое умножение задаёт структуру ассоциативной алгебры на пространстве

$$T(V) = \bigoplus_{p,q \geq 0} V^{p,q},$$

которое называется тензорной алгеброй пространства V.

Посмотрим теперь на пространство $V^* \otimes V$. Определим из него каноническое, то есть не зависящее от выбора базиса отображение в K. Действительно элементы этого пространства есть суммы тензоров вида $f \otimes v$. Сопоставим каждому такому тензору

$$(f, v) \to f(v).$$

Такое сопоставление продолжается до линейного отображения

$$Conv\colon V^* \otimes V \to K.$$

Что это за отображение в координатах? Тензор типа $(1,1)$ записывается в базисе как $T = \sum_{i,j} T^i_j e^j \otimes e_i$. Тогда

$$Conv(T) = \sum_{i,j} T^i_j e^j(e_i) = \sum_i T^i_i.$$

Если вспомнить, что пространство $V^* \otimes V \cong \mathrm{Hom}(V, V)$, то указанное отображение становится просто отображением следа. Это ещё один способ доказать инвариантность следа. Обозначение $Conv$ взято благодаря слову «convolution», то есть свёртка. Сейчас мы проделаем аналогичную конструкцию в более общем случае.

Определение. Рассмотрим пространство $V^{p,q}$ и пару индексов $j \leq p$ и $i \leq q$. Тогда свёрткой по индексам i, j называется линейное отображение

$$Conv_{i,j}\colon V^{p,q} \to V^{p-1,q-1},$$

заданное по правилу

$$\cdots \otimes f^j \otimes \cdots \otimes v_i \otimes \cdots \to f^j(v_i) \cdot f^1 \otimes \ldots.$$

Это одно из самых часто используемых понятий про тензоры. В координатном виде это просто сумма по совпадающим индексам в позиции j и i. Понятно, что свёртку можно делать по одинаковым по размеру упорядоченным группам координат. Я не буду про это говорить дополнительно.

0.22. Внешняя и симметрическая степень...

Примеры. Лемма о проекторе для внешней степени. Формулировка для симметрической степени.

Определение. Определим пространство $\Lambda^k V$ как подпространство $V^{\otimes k}$. Это подпространство выделяется следующими условиями – для любой перестановки из $\sigma \in S_k$ и любого тензора $a \in \Lambda^k V$ верно, что $\sigma(a) = \mathrm{sgn}(\sigma) a$. Под $\sigma(a)$ подразумевается действие перестановки σ на тензор a перестановкой его компонент. Аналогично определяется подпространство $\mathrm{Sym}^k V \leq V^{\otimes^k}$, чьи элементы удовлетворяют свойству: $\sigma(a) = a$.

Факт. Полезно смотреть не на пространства $\Lambda^k(V)$ и $\mathrm{Sym}^k V$, а на пространства $\Lambda^k(V^*)$ и $\mathrm{Sym}^k(V^*)$, потому что они допускают привычную и наглядную интерпретацию — их элементы это полилинейные функции со специальными свойствами.

Примеры:
1) Элемент $\Lambda^2(V^*)$ — это просто кососимметрическая билинейная форма.
2) А элемент $\mathrm{Sym}^2 V^*$ – это симметрическая билинейная форма или просто квадратичная форма.
3) Элемент $\Lambda^{\dim V} V^*$ – это просто форма объёма на V.
4) Заметим, что продолжая аналогию с квадратичными формами, выбор базиса задаёт изоморфизм

$$\mathrm{Sym}^k V^* \cong K[x_1, \ldots, x_n]_{\deg = k}$$

с пространством однородных многочленов степени k (n – размерность пространства). Последнее отображение устроено следующим образом – элементу $a \in \operatorname{Sym}^k V^*$ сопоставим отображение, которое на векторе $v = x_1e_1 + \cdots + x_ne_n$ выдаёт $a(v, \ldots, v)$. То есть

$$a \to (v \to a(v, \ldots, v)).$$

Это будет однородный многочлен от координатных функций $x_1, \ldots, x_n$. Осталось заметить, что проекция тензора $e^{i_1} \otimes \cdots \otimes e^{i_k}$ после применения такой операции — это многочлен $x_{i_1} \ldots x_{i_k}$.

Лемма 13. Имеет место проектор $Alt\colon V^{\otimes k} \to \Lambda^k V$ заданный формулой

$$a \to \frac{1}{k!} \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma)\sigma(a).$$

Аналогично отображение

$$S\colon a \to \frac{1}{k!} \sum_{\sigma \in S_k} \sigma(a)$$

есть проектор на подпространство $\operatorname{Sym}^k V$.

Доказательство. Докажем только первую часть. Прежде всего заметим, что Alt принимает значение в подпространстве кососимметричных тензоров. Действительно

$$\tau(Alt(a)) = \frac{1}{k!} \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma)\tau(\sigma(a)) = \operatorname{sgn}\tau \frac{1}{k!} \sum_{\tau\sigma \in S_k} \operatorname{sgn}(\tau\sigma)\tau(\sigma(a)) = \operatorname{sgn}(\tau)Alt(a).$$

Далее, покажем, что для любого кососимметричного тензора a верно, что $Alt(a) = a$. Это покажет, что Alt – есть проектор и в его образе лежат все элементы из $\Lambda^k(V)$, то есть ровно то, что осталось показать. Итак пусть $a \in \Lambda^k(V)$. Тогда

$$Alt(a) = \frac{1}{k!} \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma)\sigma a = \frac{1}{k!} \sum_{\sigma \in S_k} \operatorname{sgn}^2(\sigma)a = a.$$

□

0.23. Базис внешней степени. Формулировка для симметрической степени.

Определение. Пусть $e_1, \ldots, e_k$ набор элементов из V. Определим элементы $e_1 \wedge \cdots \wedge e_k \in \Lambda^k V$ как образы при проекции $e_1 \otimes \cdots \otimes e_k$.

Теорема 23. Пусть $e_1, \ldots, e_n$ базис пространства V. Тогда элементы $e_{i_1} \wedge \cdots \wedge e_{i_k}$, где $i_1 < i_2 < \cdots < i_k$ образуют базис пространства $\Lambda^k V$. В частности размерность $\dim \Lambda^k V = C_n^k$.

Доказательство. Прежде всего заметим, что это действительно порождающая система. Для этого вспомним, что $e_{i_1,\ldots,i_k}$ по всем возможным наборам $i_1, \ldots, i_k$ порождают тензорное произведение $V^{\otimes k}$. Но раз они порождают тензорное произведение, то они порождают и его образ при проекции Alt на пространство кососимметричных тензоров. Далее заметим, что

$$Alt(e_{i_1,\ldots i_k}) = \operatorname{sgn}(\sigma)Alt(e_{i_{\sigma(1)},\ldots i_{\sigma(k)}}).$$

В частности, если в наборе есть два повторяющихся индекса, то элемент проектируется в 0. Далее, это же соотношение даёт, что, возможно с точностью до знака проекция набора совпадает с проекцией упорядоченного набора. Таким образом, из набора образующих можно исключить неупорядоченные наборы и наборы с повторениями, что и требовалось.

Покажем линейную независимость. Для удобства введём обозначение: если $\Gamma \subseteq \{1, \ldots, n\}$ размера, то за e_Γ обозначим

$$e_\Gamma = e_{i_1} \wedge \cdots \wedge e_{i_k}, \text{ где } i_1 < \cdots < i_k \text{ и } \Gamma = \{i_1, \ldots, i_k\}$$

Таким образом, каждому подмножеству мы сопоставили элемент $\Lambda^k(V)$.

Пусть теперь

$$\sum_\Gamma \alpha_\Gamma e_\Gamma = 0.$$

Тогда расписывая эту сумму через базисные элементы $V^{\otimes k}$ имеем

$$\frac{1}{k!} \sum_\Gamma \alpha_\Gamma \sum_{\sigma \in S_\Gamma} \operatorname{sgn}(\sigma) e_{\sigma(i_1),\ldots,\sigma(i_k)} = 0$$

Заметим, что все слагаемые соответствуют разным базисным элементам. Тогда, все коэффициенты равны нулю. В частности, коэффицинеты при $e_{i_1,\ldots,i_k}$, которые равны $\frac{1}{k!}\alpha_\Gamma$.

□

Теорема 24. Аналогично, пусть $e_1, \dots, e_n$ базис пространства V. Тогда элементы образы тензоров $e_{i_1} \otimes \dots \otimes e_{i_k}$, где $i_1 \le \dots \le i_k$ образуют базис пространства $\operatorname{Sym}^k V$.

0.24. Внешняя степень линейного отображения. Универсальное свойство внешней степени.

Определение. Определим k-ую внешнюю степень линейного отображения $L\colon V \to W$ – отображение $\Lambda^k L\colon \Lambda^k V \to \Lambda^k W$ заданное на тензорах по правилу $v_1 \wedge \dots \wedge v_k \to Lv_1 \wedge \dots \wedge Lv_k$.

Для того, чтобы показать корректность такого определения покажем следующую теорему:

Теорема 25. Рассмотрим отображение $g = Alt \circ i\colon V^{\times k} \to \Lambda^k(V)$. Тогда для любого полилинейного кососимметрического $h\colon V^{\times k} \to U$ существует единственное отображение $\hat{h}\colon \Lambda^k(V) \to U$, что $\hat{h} \circ g = h$.

Доказательство. Зафиксируем подходящее $h\colon V^{\times k} \to U$. Так как это полилинейное отображение, то есть линейное $\hat{\hat{h}}\colon V^{\otimes k} \to U$, что $\hat{\hat{h}} \circ i = h$. Покажем, что ограничение $\hat{\hat{h}}$ на $\Lambda^k(V)$ есть искомое отображение. Действительно

$$\hat{\hat{h}}(v_1 \wedge \dots \wedge v_k) = \hat{\hat{h}}\left(\frac{1}{k!}\sum_{\sigma \in S_k} \operatorname{sgn}(\sigma) v_{\sigma(1)} \otimes \dots \otimes v_{\sigma(k)}\right) = \frac{1}{k!}\sum_{\sigma \in S_k} \operatorname{sgn}(\sigma) h(v_{\sigma(1)}, \dots, v_{\sigma(k)}) = \frac{1}{k!} k! h(v_1, \dots, v_k) = h(v_1, \dots, v_k).$$

Осталось показать единственность. Для этого заметим, что из условия $\hat{h}$ однозначно задано на базисе e_Γ. □

0.25. Внешняя алгебра и её свойства. Формулировка для симметрического случая.

Теорема 26 (Внешняя алгебра)**.** Рассмотрим пространства $\Lambda(V) = \oplus_{k=0}^{\dim V} \Lambda^k(V)$ и введём на нём структуру ассоциативной алгебры по правилу $f \wedge g = Alt(f \otimes g)$. Если $f \in \Lambda^p(V)$, а $g \in \Lambda^q(V)$, то $f \wedge g = (-1)^{pq} g \wedge f$. Такое свойство называется градуированной коммутативностью. Более того, пара $v_1 \wedge \dots \wedge v_p, u_1 \wedge \dots \wedge u_q$ переходит при этом умножении в $v_1 \wedge \dots \wedge v_p \wedge u_1 \wedge \dots \wedge u_q$. Такое умножение называется внешним произведением тензоров.

Доказательство. Для этого удобно проверить тождество $Alt(Alt(T_1) \otimes T_2) = Alt(T_1 \otimes T_2) = Alt(T_1 \otimes Alt(T_2))$, которое говорит, что внутри альтернирования можно свободно альтернировать сомножители не боясь ничего поменять. Действительно

$$\frac{1}{k!}\sum_{\sigma \in S_k} \operatorname{sgn}(\sigma) Alt(T_1^\sigma \otimes T_2) = \frac{1}{k!}\sum_{\sigma \in S_k} \operatorname{sgn}^2(\sigma) Alt(T_1 \otimes T_2) = Alt(T_1 \otimes T_2).$$

Аналогично получается второе равенство. Теперь видно, что

$$Alt(v_1 \wedge \dots \wedge v_p \otimes u_1 \wedge \dots \wedge u_q) = Alt(v_1 \otimes \dots \otimes v_p \otimes u_1 \wedge \dots \wedge u_q) = Alt(v_1 \otimes \dots \otimes v_p \otimes u_1 \otimes \dots \otimes u_q) = v_1 \wedge \dots \wedge v_p \wedge u_1 \wedge \dots \wedge u_q.$$

Это показывает связь нашего определения умножения с ожидаемым определением. Ассоциативность теперь легко проверить на базисных элементах, как и градуированную коммутативность. □

Теорема 27 (Симметрическая алгебра)**.** Рассмотрим пространство $\operatorname{Sym}(V) = \oplus_k \operatorname{Sym}^k(V)$. Тогда на нём можно ввести структуру ассоциативной коммутативной алгебры задав умножение как $f * g = S(f \otimes g)$. Более того, указанная алгебра изоморфна алгебре многочленов.

0.26. Определитель. Формула Бине-Коши.

Необработанная версия из конспекта Константина Михайловича

Покажем способ применения внешней степени для доказательства тождеств про определители. Прежде всего пусть есть отображение $L\colon U \to V$, где $\dim U = \dim V = n$ и A матрица L в базисах $e_1, \dots e_n$ и $f_1, \dots, f_n$. Тогда

$$\Lambda^n L(e_1 \wedge \dots \wedge e_n) = \det A \; f_1 \wedge \dots \wedge f_n.$$

Из этого замечания уже легко получить мультипликативность определителя. Поступая аналогично можно доказать более общую теорему:

Определение. Пусть A – матрица из $M_{m \times n}(K)$. Тогда если $\Gamma \subseteq \{1, \dots, n\}$. Тогда за A_Γ обозначим матрицу состоящую из столбцов матрицы A с элементоами из Γ.

Аналогично, если $\Gamma \subseteq \{1, \dots, m\}$ то за A^Γ обозначим подматрицу A, из строк, чьи индексы лежат в Γ.

Теорема 28 (Формула Бине-Коши)**.** Рассмотрим две матрицы $A \in M_{m\times n}(K)$ и $B \in M_{n\times m}(K)$. Пусть $m \le n$. Тогда

$$\det(AB) = \sum_{\substack{\Gamma\subseteq\{1,\dots,n\}\\|\Gamma|=m}} \det A_\Gamma \det B^\Gamma.$$

Доказательство. Рассмотрим линейный отображения заданные матрицей $B\colon K^m \to K^n$ и $A\colon K^n \to K^m$. Тогда $\det AB = \Lambda^m(AB)$ как операторы из $K \to K$. С другой стороны $\Lambda^m(AB) = \Lambda^m(A)\Lambda^m(B)$. Вычислим матрицы этих отображений. Матрица $\Lambda^m(B)$ есть столбец высоты C_n^m, чьи элементы проиндексированны $\Gamma \subseteq \{1,\dots,n\}$ размера m. Аналогично матрица $\Lambda^m(A)$ есть строчка, чьи элементы проиндексированны аналогично. Пусть $e = e_1 \wedge \dots \wedge e_m$ единственный базисный элемент $\Lambda^m(K) \cong K$, а $f_1,\dots,f_n$ – стандартный базис K^n. Тогда

$$\Lambda^m(B)e = \sum_{i_1,\dots,i_m} B_{i_1 1}\dots B_{i_m m}\, f_{i_1}\wedge\dots\wedge f_{i_m} = \sum_{\substack{\Gamma\subseteq\overline{1,n}\\|\Gamma|=m}} \sum_{\sigma\colon \overline{1,m}\to\Gamma} B_{\sigma(1)1}\dots B_{\sigma(m)m}\,\operatorname{sgn}\sigma\, f_\Gamma.$$

Здесь под знаком σ подразумевается знак перестановки, если перенумеровать элементы Γ по порядку. Теперь заметим, что при f_Γ коэффициент в точности $\det B^\Gamma$. С другой стороны, аналогично первому вычислению с определителем

$$\Lambda^m(f_\Gamma) = \det(A_\Gamma)e.$$

Осталось перемножить строчку на столбец. □

0.27. Лемма Гаусса. Содержание многочлена...

Лемма Гаусса. Содержание многочлена. Делимость в $Q(R)[x]$ и в $R[x]$.

Шпаргалка:

Лемма: Пусть нет, возьмём $\min a_i, b_j \not\vdots p$, тогда $c_{i+j} \not\vdots p$. Следствие: поделим на $\operatorname{cont} g, h$, убедимся что $\operatorname{cont} f = 1$. Лемма про $Q(R)[x]$: d_1, d_2 — НОК знаменателей, $c = \frac{d_1}{d_2}$.

Определение. Область целостности R называется **факториальным кольцом**, если для любого $a \neq 0 \in R$ существует представление a в виде $a = \varepsilon p_1 \dots p_n$, где $\varepsilon \in R^*$, а p_i — простые.
Причём такое представление единственно с точностью до ассоциированности и перестановки сомножителей. То есть для любого другого разложения $a = \varepsilon q_1 \dots q_m$ верно, что $n = m$ и существует перестановка $\sigma \in S_n q_i \sim p_{\sigma(i)}$

Лемма 14 (Гаусс)**.** Пусть R – факториальное кольцо. Тогда любой простой элемент p из R остаётся простым в $R[x]$.

Доказательство. Их будет два:

- Теоретическое
  Элемент p — простой, если идеал (p) в $R[x]$ простой, т. е. $R[x]/(p)$ — область целостности.
  (p) — идеал вида $pR[x]$, т. е. он состоит из многочленов, все элементы которых кратны p. Тогда понятно, что $R[x]/(p) = R/p[x]$. R/p — область целостности, ну а колько многочленов над областью целостности тоже область целостности.

- И практическое
  Формально нам надо доказать, что если произведение двух многочленов $f(x)g(x)$ делится на p (то есть все коэффициенты кратны p), то тогда какой-то из них делится на p. Пусть это не так. Возьмём тогда у f и у g самые младшие коэффициенты a_i и b_j, которые не делятся на p. Тогда посмотрим на коэффициент с номером $i+j$ в произведении. Он имеет вид $c_{i+j} = a_i b_j + \sum_{k\neq i} a_k b_{i+j-k}$. Поймём, что c_{i+j} не делится на p: $a_i b_j$ не делится на p, а любое слагаемое в сумме делится, так как либо $k < i$ и тогда $a_i \vdots p$, либо $k > i$, тогда $i+j-k < j$ и $b_j \vdots p$. Противоречие.

□

Определение. Пусть $f(x)$ – многочлен над факториальным кольцом R. Тогда содержанием f называется $\operatorname{cont}(f) =$ НОД(a_i), где a_i коэффициенты f.
(Помним, что НОД определён с точностью до ассоциированности.)

Следствие 2. (из Леммы Гаусса)
Если $f(x) = g(x)h(x)$, где $f, g, h \in R[x]$, то $\operatorname{cont}(f) = \operatorname{cont}(g)\operatorname{cont}(h)$

Доказательство. Для начала, упростим задачу, то есть сведём задачу к случаю $\operatorname{cont} g = \operatorname{cont} h = 1$. Для этого надо рассмотреть многочлены $\frac{g}{\operatorname{cont} g}$ и $\frac{h}{\operatorname{cont} h}$. Их произведение есть $\frac{f}{\operatorname{cont} g \operatorname{cont} h}$ имеет содержание $\frac{\operatorname{cont} f}{\operatorname{cont} g \operatorname{cont} h}$ и если показать его единичность, то мы добьёмся требуемого. Итак считаем, что $\operatorname{cont} g = \operatorname{cont} h = 1$. Если $\operatorname{cont} f$ не обратим, то $\operatorname{cont} f \vdots p$, где p простой элемент из R. Но тогда один из g или h делится на p благодаря его простоте. □

Вспомним, что для полей мы знаем про однозначность разложения. Так что внимальтельнее посмотрим на поле частных $Q(R)$.

Лемма 15. Пусть для многочлена $f(x) \in R[x]$ имеет место разложение $f(x) = g(x)h(x)$, где $g(x)h(x) \in Q(R)[x]$. Тогда существуют такая константа $c \in Q(R)$, что $cg \in R[x]$ и $c^{-1}h \in R[x]$. Так что $f(x) = (cg(x))(c^{-1}h(x))$ – есть произведение двух многочленов из $R[x]$, пропорциональных исходным.

Доказательство. Рассмотрим несократимую запись для коэффициентов g и h и НОК их знаменателей за d_1 и d_2 соответственно. Тогда $d_1 g$ и $d_2 h$ лежат в $R[x]$. Получаем равенство $d_1 d_2 f = (d_1 g)(d_2 h)$. Посчитаем содеражание слева и справа: $d_1 d_2 \operatorname{cont} f = \operatorname{cont}(d_1 g) \operatorname{cont}(d_2 h)$. Таким образом, правая часть делится на $d_1 d_2$. Вспомним как мы выбирали d_1 и поймём, что $(\operatorname{cont}(d_1 g), d_1) = 1$ (аналогично про d_2). Значит $\operatorname{cont}(d_1 g) \vdots d_2$ и $\operatorname{cont}(d_2 h) \vdots d_1$. Возьмём теперь $c = \frac{d_1}{d_2}$ и победим. □

0.28. Факториальность кольца многочленов над факториальным кольцом.

Шпаргалка:
$R[x]$ факториально и простые в нём: $f = p \in R$, $f : \operatorname{cont}(f) = 1$ — непр. в $Q(R)[x]$. Док-во: 1) они и правда простые 2) в них раскладывается (посмотрим в $Q(R)$) 3) единственность ⇒ других нет

Теорема 29. Пусть R – факториальное кольцо. Тогда кольцо $R[x]$ факториально. Более того, имеет место следующее описание простых элементов кольца $R[x]$:
1) $f = p \in R$ – простой в R.
2) $\operatorname{cont}(f) = 1$ и f неприводим в $Q(R)[x]$.

Доказательство. Для начала покажем, что все указанные ситуации приводят к простым элементам в кольце $R[x]$ и что других простых и, более того, неприводимых не бывает.

Почему просты элементы первого типа, говорит лемма Гаусса. Про второй: возьмём $f \in R[x]$ неприводим в $Q(R)[x]$. Если $gh \vdots f$, то это же верно над $Q(R)$ и, можно считать например, что $g \vdots f$ в $Q(R)[x]$. Тогда $g = fk$. Теперь можно домножить на подходящую константу $g = (cf)(c^{-1}k)$ чтобы получить равенство в $R[x]$. Заметим, что $c(c^{-1}k)$ из $R[x]$, что показывает, что $g \vdots f$ в $R[x]$, а занчит f прост в $R[x]$.

Покажем, что любой элемент раскладывается в произведение тех простых, что мы описали. Для этого сначала разложим f в $Q(R)[x]$ в произведение неприводимых $f = \prod g_i$, $g_i \in Q(R)[x]$. Далее сделаем из g_i элементы $\hat{g}_i$ из $R[x]$ с $cont(g_i) = 1$, что $f = a \prod \hat{g}_i$. Заметим, что $a = cont(f)$ и, следовательно, лежит в R. Итого $f = a \prod \hat{g}_i$, где $0 \neq c \in R$. Осталось разложить c (в простые первого типа).

Осталось показать единственность. Это следует лишь из того, что у нас есть разложение на простые. Действительно, если $f = \prod p_i = \prod q_i$, то $p_i \mid \prod q_i$ и, благодаря простоте, делит какое-то q_i. Но тогда $p_i h = q_i$, откуда, по неприводимости q_i, получаем, что h обратим, то есть, что $p_i \sim q_i$. Тогда можно сократить на p_i и продолжить по индукции.

Отсутствие простых, отличных от указанных типов, следует теперь из единственности разложения. □

•

0.29. Редукционный признак неприводимости. Примеры. Признак Эйзенштейна.

Шпаргалка.
1) $a_n \not\vdots p$, f - неприводим в $R/p[x]$ ⇒ неприводим над $Q(R)$. $cont = 1$ и неприводимость над $Q(R)$ ⇒ неприводимость над R. 2) $a_n \not\vdots p$, все $a_i \vdots p$ $i < n$, но $a_0 \not\vdots p^2$, то многочлен $f(x)$ неприводим. Пусть $b_0 \not\vdots p$.

Теорема 30 (Редукционный критерий)**.** Пусть R факториальное кольцо, $f \in R[x]$ многочлен, а p – простой элемент. Тогда, если старший коэффициент f не делится на p и $\overline{f}$ неприводим в кольце $R/p[x]$, то он неприводим над $Q(R)$.

Доказательство. Хотим пользоваться тем, что при каких-то условиях неприводимость над R эквивалентна неприводимости над $Q(R)$. Стрелка в правую сторону очевидна. Можно поделить f на $cont(f)$, чтобы воспользоваться знаниями из предыдущего билета о том, что неприводимые многочлены над $Q(R)$, чье содержание равно единице, - это все неприводимые многочлены в $R[x]$(так было на лекции). Кажется, что проще воспользоваться леммой из предыдущего билета о том, что если есть разложение на два многочлена из $Q(R)[x]$, то есть разложение и на два многочлена из $R[x]$. Теперь можно доказывать теорему для R. Пусть $f = gh$, где g, h – не константы. Старшие коэффициенты g и h тоже не делятся на p. Имеем $\overline{f} = \overline{g}\overline{h}$ и $\deg g = \deg \overline{g}$ и $\deg h = \deg \overline{h}$, что даёт нетривиальное разложение $\overline{f}$ и приводит к противоречию. □

Вот примеры о том, как пользоваться этим критерием и что не надо забывать про условие со старшим коэффициентом.

Примеры:

1) Многочлен x^3+x+1 неприводим над $\mathbb{F}_2 = \mathbb{Z}/2$, потому что у него нет корней. Следовательно многочлены $3x^3+8x^2+5x+7$ и скажем, $5x^3-4x^2+x+15$ неприводимы над $\mathbb{Q}$.

2) Рассмотрим многочлен px^2+x. Он приводим, но по модулю p – неприводим.

3) Критерий из теоремы сформулирован не в самом сильном виде. А именно, представим себе, например, что по модулю 2 многочлен степени пять разложился в произведение двух неприводимых степени 2 и 3, а по модулю 3 – в виде произведения степени 4 и 1. Ясно, что он неприводим.

4) Не стоит забывать, что если многочлен неприводим над $\mathbb{R}$, то он так же неприводим над $\mathbb{Q}$. Это, правда, очень слабый критерий, но в комбинации с пунктом 3) может что-то дать.

Есть, однако, такие многочлены, которые неприводимы, но раскладываются по модулю любого простого. Например,

$$x^4+1 = (x-e^{\frac{i\pi}{8}})(x-e^{\frac{3i\pi}{8}})(x-e^{\frac{5i\pi}{8}})(x-e^{\frac{7i\pi}{8}}) = (x^2+i)(x^2-i) = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1) = (x^2+\sqrt{-2}x+1)(x^2-\sqrt{-2}x+1).$$

Он не имеет корней, а любые множители степени 2 имеют нерациональный коэффициент.

С другой стороны по любому простому модулю либо из -1, либо из 2 либо из -2 извлекается корень.

Комментарии к последнему примеру: на лекциях его не было, и последнее утверждение не за одну секунду доказывается.

Теорема 31 (Признак Эйзенштейна)**.** Пусть R – факториальное кольцо и $f(x) = a_0 + \cdots + a_n x^n$. Если $a_n \not\vdots p$, все $a_i \vdots p$ $i < n$, но $a_0 \not\vdots p^2$, то многочлен $f(x)$ неприводим.

Доказательство. Предположим, что $f = gh$. Заметим, что старшие коэффициенты b_k и c_l у g и h не делятся на p. Пусть так же $b_0 \not\vdots p$ у многочлена g. Рассмотрим самый младший коэффициент у h не делящийся на p. Такой есть, потому что $c_l \not\vdots p$ и это точно не c_0. Пусть это c_s. Тогда $a_s = c_s b_0 + c_{s-1} b_1 + \cdots + c_0 b_s$. Все слагаемые, кроме первого делятся на p. Но тогда $a_s \not\vdots p$, что невозможно. □

0.30. Алгоритм Кронекера. Сведение для многочленов от нескольких переменных.

Шпаргалка.

1) Перебираем наборы делителей $f(i)$, $0 \le i \le \frac{degf}{2}$, интерполируем, проверяем. 2) Различным разложениям $f(x_1, \ldots, x_n)$ соответствуют различные разложения $f(x, \ldots, x^{d^{n-1}})$ для d больших $\max_{i=1}^{n}\{\deg_{x_i} f\}$. Рассмотреть образ x^α.

Алгорим Кронекера

Итак, пусть есть целочисленный многочлен $f(x)$ и мы хотим разложить его на множители. Мы будем искать разложение на целочисленные многочлены, заметим, что хотя бы один из них имеет степень меньшую, чем $[\frac{n}{2}]$. Вспомним о задаче интерполяции. Если g – искомый делитель f, то g определяется своими значениями в $[\frac{n}{2}]+1$ точке, например в точках $0, 1, \ldots, [\frac{n}{2}]$. Более того, $f(i) \vdots g(i)$. Таким образом набор $g(0), \ldots, g([\frac{n}{2}])$ состоит из делителей $f(0), \ldots, f([\frac{n}{2}])$. Найти все такие наборы – конечный перебор. По каждому набору восстановим g по интерполяции и проверим, является ли он делителем f.

Сведем задачу разложения многочленов от нескольких переменных к предыдущей.

Теорема 32. Пусть R – кольцо. Тогда различным разложениям $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ соответствуют различные разложения $\hat{f} = f(x, x^d, x^{d^2}, \ldots, x^{d^{n-1}})$ для d больших $\max_{i=1}^{n}\{\deg_{x_i} f\}$.

Доказательство. Пусть $f = g_1 h_1 = g_2 h_2$ и пусть $g_1 \neq g_2$. Покажем, что $\hat{g_1} \neq \hat{g_2}$. Мы рассматриваем отображение $f(x_1, \ldots, x_n) \to f(x, x^d, \ldots, x^{d^{n-1}})$. Рассмотрим мономом x^α, где α - это мультииндекс. Он переходит в многочлен $x^{\alpha_1+\alpha_2 d+\cdots+\alpha_n d^{n-1}}$. По условию все $\alpha_i < d$ как степени при переменных x_i. Тогда моном $x^{\alpha_1+\alpha_2 d+\cdots+\alpha_n d^{n-1}}$ может быть получен только из монома x^α. Заметим теперь, что $\deg_{x_i} g_j \le \deg f < d$. Следовательно мономы многочленов $g_j(x)$ так же однозначно восстанавливаются по мономам $\hat{g_j}$. □

К сожалению, не стоит ожидать взаимооднозначного соответствия между разложениями многочленов f и $\hat{f}$. Например, многочлен x_2^2 раскладывается на два множителя одним способом. При $d = 3$ его образ есть x^6 у которого 3 различных разложения.

0.31. Лемма Гензеля. Разложение на множители при помощи леммы Гензеля.

Шпаргалка.
Доказательство леммы: Индукция по k. Строим для k + 1. Помним, что $\forall f:\ p^k f \equiv p^k \overline{f} \pmod{p^{k+1}}$.
$\overline{h} \equiv \hat{h} + p^k a(x) \Rightarrow \overline{h}\overline{g} \equiv \hat{g}\hat{h} + p^k(a(x)g + b(x)h)$. С другой стороны $f - \hat{g}\hat{h} = p^k c(x) \Rightarrow a,\ b$ берем из лп НОДа g и h

Теперь вернёмся к многочленам от одной переменной. Для проверки неприводимости мы с успехом использовали информацию, полученную из разложения по модулю n. Вопрос – нельзя ли её же использовать и в целочисленной задаче?

Во-первых, если взять достаточно большой модуль n, заметно больший, чем коэффициенты в целочисленном разложении, то разложение f по модулю n с маленькими коэффициентами однозначно будет определять кандидата на целочисленное разложение. Это соображение встречается сразу с двумя проблемами – первая – не ясно какие есть ограничения на коэффициенты сомножителей, вторая – разложений по модулю n может быть много и нет способа эффективно искать их.

Как же теперь выбрать достаточно большое число, по модулю которого раскладывать многочлен f на множители? В первую очередь, должно быть удобно раскладывать многочлен по подходящему множителю. Наибольшим удобством в решении задачи разложения обладают поля. В этом смысле возможно стоило бы искать разложение f по модулю очень большого простого. Однако найти большое простое число довольно тяжело. Смотреть по модулю маленьких простых а потом пытаться склеивать разложение в духе китайской теоремы об остатках может банально не получиться (как в примере 3 из билета 29 – неясно во что склеить два разных разложения). Оказывается наиболее оптимальный вариант такой – взять небольшое простое число p, разложить f над $\mathbb{Z}/p$ а затем «поднять» это разложение по модулю p^k для достаточно большого k. Сформулируем утверждение, которое пояснит как это сделать.

Замечание. Пусть $f \in \mathbb{Z}[x], \overline{f} \in \mathbb{Z}/p[x] \Rightarrow p^k f \equiv p^k \overline{f} \pmod{p^{k+1}}$

Доказательство. Посмотрим на $a_i \in f$.

$$p^k a_i \equiv p^k(pq_i + r_i) \equiv p^{k+1}q_i + p^k r_i \equiv p^k r_i \equiv p^k \overline{a_i} \pmod{p^{k+1}}$$

□

Лемма 16 (Гензеля)**.** Пусть $f \in \mathbb{Z}[x]$, со старшим коэффициентом не делящимся на простое число p. Пусть $\overline{f} = gh$ в кольце $\mathbb{Z}/p[x]$, причём $(g,h) = 1$. Тогда для любого $k \geq 1$ существуют единственные по модулю p^k многочлены $\hat{g}, \hat{h} \in \mathbb{Z}[x]$, что $\overline{f} = \hat{g}\hat{h} \bmod p^k$ и $\deg h = \deg \hat{h}$, $\deg g = \deg \hat{g}$, $\hat{g} \equiv g \pmod{p}$, а $\hat{h} \equiv h \pmod{p}$.

Доказательство. Докажем это индукцией по k. Пусть по модулю p^k уже построены подходящие многочлены $\hat{h}$ и $\hat{g}$ и мы хотим построить $\overline{h}$ и $\overline{g}$. Заметим, что благодаря единственности по модулю p^k, такие $\overline{g}$ и $\overline{h}$ обязаны совпадать с $\hat{h}$ и $\hat{g}$ по модулю p^k. Это означает, что по модулю p^{k+1}

$$\overline{h} \equiv \hat{h} + p^k a(x) \pmod{p^{k+1}} \quad \text{и} \quad \overline{g} \equiv \hat{g} + p^k b(x) \pmod{p^{k+1}}.$$

Заметим, что многочлены $a(x)$ и $b(x)$ однозначно определяются по модулю p (по прошлому замечанию), если известны $\overline{g}$ и $\overline{h}$ и по модулю p могут иметь степени меньше чем степени $h(x)$ и $g(x)$ соответственно. Покажем, что такие $a(x), b(x)$ существуют и единственны по модулю p. Заметим, что необходимо проверить лишь условие $f \equiv \overline{g}\overline{h} \pmod{p^{k+1}}$. Распишем

$$f \equiv \hat{g}\hat{h} + a(x)p^k\hat{g} + b(x)p^k\hat{h} + p^{2k}a(x)b(x) \equiv \hat{g}\hat{h} + p^k(a(x)g + b(x)h) \pmod{p^{k+1}}.$$

Здесь мы заменили $\hat{h}$ и $\hat{g}$ по модулю p (опять по прошлому замечанию) и получили исходные многочлены g и h из $\mathbb{Z}/p[x]$. Заметим, что есть единственный такой многочлен $c(x) \in \mathbb{Z}/p[x]$, что $f - \hat{g}\hat{h} = p^k c(x) \pmod{p^{k+1}}$. Теперь для выполнения сравнения выше необходимо, чтобы

$$c(x) = a(x)g(x) + b(x)h(x)$$

У такого сравнения есть единственное решение в $\mathbb{Z}/p[x]$ (лп НОДа) при условиях $(g,h) = 1$ и $\deg a(x) < \deg h(x)$ и $\deg b(x) < \deg g(x)$. Что и требовалось. □

Частным случаем разложения на множители служит разложение вида $f(x) = (x - x_1)g(x)$, соответствующее наличию корня. Сформулируем следствие леммы Гензеля в этой ситуации:

Следствие 3. Пусть $f \in \mathbb{Z}[x]$, со старшим коэффициентом не делящимся на простое число p. Пусть a корень f по модулю p, причём $\overline{f}'(a) \neq 0$. Тогда для любого $k \geq 1$ существует единственный $\hat{a} \in \mathbb{Z}/p^k$, что $f(\hat{a}) = 0$ и $\hat{a} \equiv a \bmod p$.

Доказательство. a корень f по модулю $p \Rightarrow \overline{f} \equiv (x-a)h(x) \pmod p$.
$\overline{f}'(a) \neq 0 \Rightarrow a$ не кратный корень $\Rightarrow ((x-a), h(x)) = 1$, значит можем применить лемму Гензеля. □

Замечание. Можно усилить лемму Гензеля, рассматривая подъём разложения не с модуля p, а с модуля p^k заработав ослабление условия на производную.

Теперь алгоритм разложения на множители уже вырисовывается (описан перед леммой). Но в лемме Гензеля есть некоторые ограничения на разложение многочлена $\overline{f}$. Как с этим жить мы узнаем дальше.

Спойлер:
Дискриминант даёт ответ на вопрос, когда многочлен не имеет кратных корней по модулю p. Действительно это происходит только тогда, когда $D(f) \not\vdots p$. Заметим, что это условие может нарушаться только в конечном числе p, если $D(f) \neq 0$. Таким образом либо у многочлена есть кратный корень, либо у него нет кратных корней для почти всех p. Это обосновывает, что для применения леммы Гензеля для подъёма всегда можно выбрать подходящее простое, если многочлен f был бесквадратный.

0.32. Степенные суммы. Тождество Ньютона.

Шпаргалка: $0 = (-1)^n n\sigma_n + \sum_{k=0}^{n-1}(-1)^k \sigma_k s_{n-k}$, в многочлен подставим корни, просуммируем по всем корням, отдельно случаи $k < n$ - добавим нулевые переменные, $k > n$ - занулим не входящие в моном переменные

Степенная сумма
$s_k(x_1, \ldots, x_n) = x_1^k + \cdots + x_n^k$

Элементарная симметрическая функция
Функция $\sigma_k(x_1, \ldots, x_n) = \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} \ldots x_{i_k}$ называется элементарной однородной степени k симметрической функцией от переменных $x_1, \ldots, x_n$. Если многочлен $p(x) = (x - x_1)\ldots(x - x_n) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, то $a_i = (-1)^{n-i}\sigma_{n-i}(x_1, \ldots, x_n)$.

Тождество Ньютона
Степенные суммы и элементарные симметрические многочлены связаны тождествами

$$0 = (-1)^n n\sigma_n + \sum_{k=0}^{n-1}(-1)^k \sigma_k s_{n-k}$$

Доказательство
1. Докажем равенство, если число переменных равно n
Рассмотрим равенство

$$(x - x_1)\ldots(x - x_n) = x^n + \sum (-1)^{n-i}\sigma_{n-i}x^i.$$

Равенство верно по определению σ_{n-i}
Подставим в это равенство $x = x_j$. Получим

$$0 = x_j^n + \sum (-1)^{n-i}\sigma_{n-i}x_j^i.$$

Просуммируем по всем j. Получим

$$0 = s_n + \sum_{i \neq 0}(-1)^{n-i}\sigma_{n-i}s_i + (-1)^n n\sigma_n$$

Так как $\sum_j x_j^i = s_i$
Это доказывает равенство, когда число переменных равно номеру σ_n. Подставив переменные $x_{k+1}, \ldots, x_n$ равные 0 в это равенство получим его для k переменных $k < n$.
Теперь предположим, что $k > n$. Проверим, что справа и слева однинаковые мономы входят с одинаковым коэффициентом. Заметим, что в каждом мономе заведомо участвует не более n различных переменных так степень каждого монома ровно n. Пусть мы хотим проверить наличие справа и слева одинакового числа мономов в записи которых участвуют переменные $x_{i_1}, \ldots, x_{i_n}$. Подставим вместо всех остальных переменных 0. Понятно, что с искомым мономом ничего не произойдёт. С другой стороны после такой подстановки и переобозначения переменных мы приходим к уже доказанному равенству, когда $k = n$.

0.33. Целые алгебраические элементы. Замкнутость относительно операций.

Шпаргалка: a алгебраический $== \exists f \in \mathbb{Z}[x] : f(a) = 0$. Замкнуто: $\prod(x - (a_i + b_j))$ симметрично по a_i, тогда коэффициенты выражаются через симметрические, симметрический по b_i - все коэффициенты целые.

Целый алгебраический элемент
Элемент $\alpha \in \mathbb{C}$ называется целым алгебраическим или просто целым, если существует такой многочлен $f(x) \in \mathbb{Z}[x]$, что $f(\alpha) = 0$ и при этом $f \neq 0$ и старший коэффициент f равен 1.

Теорема. Сумма целых элементов цела и произведение целых элементов цело.
Доказательство
Пусть α и β – целые, а $f(x) = a_0 + \cdots + x^n$ и $g(x) = b_0 + \cdots + x^m$ – обнуляющие их целочисленные многочлены со старшим коэффициентом, равным единице. Пусть $\alpha = \alpha_1, \ldots, \alpha_n$ и $\beta = \beta_1, \ldots, \beta_m$. Тогда рассмотрим многочлен

$$\prod_{i,j}(x - (\alpha_i + \beta_j))$$

его корнем является $\alpha + \beta$ и он имеет старший коэффициент 1. Осталось показать, что его коэффициенты целые. Представим на секунду, что α_i и β_j – это независимые переменные. В самом конце подставим в них настоящие значения. Тогда этот многочлен симметричен по α_i в кольце $\mathbb{Z}[\beta_1, \ldots, \beta_m]$. Следовательно его коэффициенты выражаются через $a_i = \pm\sigma_{n-i}(\alpha_1, \ldots, \alpha_n)$, $\beta_1, \ldots, \beta_m$ и целые числа. Но это выражение симметрично и по β_j. Откуда коэффициенты этого многочлена выражаются через $\sigma_{n-i}(\alpha_1, \ldots, \alpha_n)$, $\sigma_{m-j}(\beta_1, \ldots, \beta_m)$ и целые числа. Теперь подставляя настоящие α_i, β_j получаем, что это многочлен с целыми коэффициентами, так как a_i и b_j целые по условию.

Аналогично, рассмотрим многочлен

$$\prod_{i,j}(x - \alpha_i\beta_j).$$

Представим на секунду, что α_i и β_j – это независимые переменные. В самом конце подставим в них настоящие значения. Тогда этот многочлен симметричен по α_i в кольце $\mathbb{Z}[\beta_1, \ldots, \beta_m]$. Следовательно его коэффициенты выражаются через $a_i = \pm\sigma_{n-i}(\alpha_1, \ldots, \alpha_n)$, $\beta_1, \ldots, \beta_m$ и целые числа. Но это выражение симметрично и по β_j. Откуда коэффициенты этого многочлена выражаются через $\sigma_{n-i}(\alpha_1, \ldots, \alpha_n)$, $\sigma_{m-j}(\beta_1, \ldots, \beta_m)$ и целые числа. Теперь подставляя настоящие α_i, β_j получаем, что это многочлен с целыми коэффициентами, так как a_i и b_j целые по условию.

0.34. Результант. Совпадение двух определений (без лемм).

шпаргалка

Пусть f и g многочлены степеней n и m. Тогда наличие общего множителя (константы не считаются) у f и g $\iff$ существование многочленов k_1 и k_2, $\deg k_1 < n$, $\deg k_2 < m$, что $fk_2 - gk_1 = 0$

Доказательство. "$\Rightarrow$"

Если есть общий множитель h, то $f = hk_1$ и $g = hk_2$. Тогда $fk_2 - gk_1 = hk_1k_2 - hk_2k_1 = 0$

"$\Leftarrow$"

Пусть такие k_1 и k_2 нашлись. Тогда $fk_2 = gk_1$. Из чего следует, что $fk_2 \vdots g$. Предположим, что g и f взаимно простые. Тогда $k_2 \vdots g$, что неверно из-за ограничения на степень k_2. Значит, g и f имеют общий множитель. $\square$

Рассмотрим отображение $K[x]_{\leq m-1} \oplus K[x]_{\leq n-1} \to K[x]_{\leq n+m-1}$, заданное по правилу

$$(k(x), l(x)) \to k(x)f(x) + l(x)g(x).$$

Данное отображение вырождено тогда и только тогда, когда есть многочлены маленьких степеней, что $k(x)f(x) = -l(x)g(x)$. По доказанному выше, это происходит тогда и только тогда, когда у многочленов f и g есть общий множитель. С другой стороны, отображение вырождено, если определитель матрицы данного отображения равен 0.

Возьмем в качестве базиса исходного пространства $1_k, x_k, x_k^2, \ldots, x_k^{m-1}, 1_l, \ldots, x_l^{n-1}$. Пусть $f(x) = a_0 + \cdots + a_nx^n$, а $g(x) = b_0 + \cdots + b_mx^m$. Тогда матрица оператора будет иметь вид:

$$\begin{pmatrix} a_0 & 0 & \cdots & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdots & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & b_m \end{pmatrix}$$

Транспонируем матрицу, переставим столбцы и, возможно, домножим на (-1):

Определение. 1 Пусть многочлен $f(x) = a_0 + \cdots + a_n x^n$, а $g(x) = b_0 + \cdots + b_m x^m$. Тогда результантом многочленов f и g называется

$$Res(f,g) = \det \begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_0 & \cdots & 0 \\ & & & & & & \\ 0 & \cdots & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 \\ b_m & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ & & & & & & \\ 0 & \cdots & 0 & b_m & \cdots & b_1 & b_0 \end{pmatrix}.$$

Эта матрица называется матрицей Сильвестра.

Определение. 2 Пусть многочлен $f(x) = a_0 + \cdots + a_n x^n$, а $g(x) = b_0 + \cdots + b_m x^m$ из кольца $K[x]$, где K – поле. Пусть так же в поле K имеются разложения $f(x) = a_n \prod(x - x_i)$, а $g(x) = b_m \prod(x - y_j)$. Тогда

$$Res(f,g) = a_n^m b_m^n \prod_{i,j}(x_i - y_j),$$

Теорема 33. Определения равны

Доказательство. $\det S$ – многочлен от коэффициентов f и g. Но каждый коэффициент многочлена, кроме старшего, – симметрический многочлен от корней. Тогда поделим $p(x_1 \ldots, x_n, y_1, \ldots, y_m) = \det S$ на $(x_i - y_j)$ с остатком как многочлен от x_i

$$p = (x_i - y_j)q + r(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n, y_1, \ldots, y_m).$$

В остатке стоит многочлен r степени 0 по x_i, то есть от x_i не зависящий. Подставим $x_i = y_j$, $Res(f,g) = \det S = p$ станут равны нулю (из того, как мы строили результант). Тогда и $r = 0$, то есть $\det S \vdots (x_i - y_j)$. Так как все $(x_i - y_j)$ взаимно просты в $R[y_0, \ldots, y_m, x_0, \ldots, x_n]$, то $\det S \vdots \prod(x_i - y_j)$.

Заметим, что мы можем рассматривать $\det S$ и $a_n^m b_m^n \prod_{i,j}(x_i - y_j)$ как многочлены над $R[a_n, b_m, y_0, \ldots, y_m, x_0, \ldots, x_n]$. Тогда $\det S$ будет все еще делиться на второе определение. (вынесем a_n из всех коэффициентов f и b_m из всех коэффициентов g в определителе. Определитель все еще будет продолжать делиться на $\prod_{i,j}(x_i - y_j)$, так как корни не изменились и предыдущие рассуждения остались верны).

Итого поняли, что $\det S$ делиться на $a_n^m b_m^n \prod_{i,j}(x_i - y_j)$ как многочлены в $R[a_n, b_m, y_0, \ldots, y_m, x_0, \ldots, x_n]$. Лемма, завершающая доказательство, в следующем билете.

□

0.35. Леммы про результант. Дискриминант, его смысл. Вычисление через результант.

Лемма 17.

$$a_n^m b_m^n \prod_{i,j}(x_i - y_j) = (-1)^{mn} b_m^n \prod f(y_j) = a_n^m \prod g(x_i).$$

Доказательство.

$$a_n^m b_m^n \prod_{i,j}(x_i - y_j) = b_m^n \prod_j (a_n \prod_i (y_j - x_i)) = (-1)^{mn} b_m^n \prod f(y_j)$$

□

Продолжение доказательства из предыдущего билета:

Подставляем формулы вида $(f(x) = a_0 + \cdots + a_n x^n)$ в лемму, понимаем, что результант есть однородный многочлен степени m из $R[a_0, \ldots, a_n]$ и степени n из $R[b_0, \ldots, b_n]$. Значит, и $\det S$ и другая формула для результанта – однородные многочлены степени $n + m$ над коэффициентами a_i и b_j. Заметим, что делимость, доказанная ранее, у нас осталась и для такого рассмотрения многочленов.

Доказательство. обозначим вторую формулу как Res'.

$\det S = Res' \cdot h$. (Как многочлены от корней). Заметим, что h тоже симметрический многочлен от корней. Поэтому выражается через коэффициенты многочленов. Значит $\det S \vdots Res'$ в $R[a_0, \ldots, a_n, b_0, \ldots, b_n]$. □

Значит, они равны с точностью до обратимого множителя. Для этого найдём коэффициент при мономе $a_n^m b_0^n$ у обоих выражений. В результанте данный коэффициент равен 1. Получаем моном $a_n^m b_0^n$ из выражения $(-1)^{mn} b_m^n \prod f(y_j)$:

$$(-1)^{mn} b_m^n a_n^m \prod_{j=1}^{m} y_j^n = (-1)^{mn} b_m^n a_n^m (-1)^{mn} \sigma_m^n = a_n^m b_m^n \sigma_m^n = a_n^m b_0^n$$

Коэффициент равен 1.

Упражнение 1. *Кроме того, если* $f = gq + r$, *где* $\deg r = k$, *то*

$$Res(f, g) = (-1)^{(n-k)m} b_m^{n-k} Res(r, g).$$

Доказательство. Доказывается подставлением первой части леммы вместо $Res(r, g)$. □

Определение. Дискриминантом многочлена $f = a_0 + \cdots + a_n x^n$ называется выражение

$$D(f) = a_n^{2n-2} \prod_{i<j} (x_i - x_j)^2.$$

Лемма 18. Имеет место равенство $Res(f, f') = (-1)^{\frac{n(n-1)}{2}} a_n D(f)$.

Доказательство. Прежде всего вспомним (дифференциируем $a_n \prod(x - x_i)$), что если $x_1, \ldots, x_n$ – корни многочлена $f(x)$, то

$$f'(x_i) = a_n \prod_{j \neq i} (x_i - x_j).$$

Посчитаем теперь пользуясь леммой из начала билета.

$$Res(f, f') = a_n^{n-1} \prod_{i=1}^{n} f'(x_i) = a_n^{2n-1} \prod_{i=1}^{n} \prod_{j \neq i} (x_i - x_j).$$

Осталось вынести знак из половины скобок слева. □

Дискриминант даёт ответ на вопрос, когда многочлен не имеет кратных корней по модулю p. Действительно это происходит только тогда, когда $D(f) \not\vdots p$. Заметим, что это условие может нарушаться только в конечном числе p, если $D(f) \neq 0$. Т аким образом либо у многочлена есть кратный корень, либо у него нет кратных корней для почти всех p. Это обосновывает, что для применения леммы Гензеля для подъёма всегда можно выбрать подходящее простое, если многочлен f был бесквадратный.

0.36. Степень расширения. Теорема о башне полей.

Определение (Степень расширения)**.** Пусть L расширение поля K (то есть K подполе в L). L можно рассматривать как векторное пространство над полем K (есть сложение элементов и умножение на элементы $\in K$). Тогда размерность данного векторного пространства $:= \dim_K L$ называется степенью L над K и обозначается как $[L : K]$. Если $[L : K]$ конечно, то говорят, что L – конечное расширение поля K.

Теорема 34 (О башне полей)**.** Пусть дана башня расширений $K \leq L \leq M$. Тогда

$$[M : K] = [M : L][L : K].$$

В частности, если M конечно над L, а L конечно над K, то M конечно над K.

Доказательство. Возьмем u_i – базис M над L, v_j – базис L над K. Докажем, что базис M над K – все возможные произведения u_i на v_j.

Докажем, что $u_i v_j$ – порождающая система. Возьмем $x \in M$. Так как u_i – базис M над L, то $x = \sum_i \lambda_i u_i$, $\lambda_i \in L$. v_j – базис L над K, поэтому $\lambda_i = \sum_j \alpha_j v_j$, $\alpha \in K$. Итого получили, что $x = \sum_i (\sum_j \alpha_{i,j} v_j) u_i = \sum_{i,j} \alpha_{i,j} u_i v_j$.

Докажем, что $u_i v_j$ линейно независимы. Пусть $\sum_{i,j} \alpha_{i,j} u_i v_j = 0$ и $\alpha_{i,j}$ не все равны 0. Тогда $\sum_i (\sum_j \alpha_{i,j} v_j) u_i = 0$. Так как u_i линейно независимы, то все коэффициенты-суммы $\sum \alpha_{i,j} v_j$ равны нулю. Но так как не все $\alpha_{i,j}$ равны нулю, то в какой-то из таких сумм есть ненулевые коэффициенты. Но в таком случае такая сумма не может равняться нулю, так как v_j – базис и, следовательно, линейно независимы.

□

Следствие 4. Пусть $[L : K]$ – конечное расширение степени n, а $[M : K]$ – степени d. Тогда, если $d \not\vdots n$, то M не может быть подрасширением L/K.

0.37. Описание наименьшего подрасширения, содержащего данный элемент.

$K(\alpha) \cong K[\alpha] \cong K[x]/p(\alpha)$, рассмотрим $K[x] \to L$, переводящий $x \to \alpha$ и $K[x]/p(x) \to L$. Следствия про равенство степеней расширения над K и изоморфность расширений для корней неприводимого многочлена.

Определение. Элемент $\alpha \in L$ называется алгебраическим над K, если существует многочлен $0 \neq p(x) \in K[x]$, что $p(\alpha) = 0$.

Теорема 35. Пусть L/K расширение полей, а $\alpha \in L$. Тогда если α алгебраическое над K, то

$$K(\alpha) = K[\alpha] \cong K[x]/p(x), \text{ где } p(x) \text{ минимальный многочлен для } \alpha.$$

Если же α не алгебраическое, то

$$K[\alpha] \cong K[x] \text{ и } K(\alpha) \cong K(x).$$

($K(x)$ – поле дробно-рациональных функций)

Доказательство. Итак, пусть α – алгебраический над $\mathbb{K}$. Тогда минимальный многочлен α однозначно определён. Покажем, что он неприводим. Пусть $p(x) = h(x)q(x)$. Тогда $h(\alpha)q(\alpha) = 0$. Но L – поле. Откуда либо $h(\alpha) = 0$ либо $q(\alpha) = 0$. Но тогда $p(x)$ не минимальный. Теперь мы знаем, что $K[x]/p(x)$ – поле.

Существует единственный гомоморфизм $K[x] \to L$, переводящий $x \to \alpha$ и оставляющих K на месте, это гомоморфизм алгебр, его ядро – $< p(x) >$. Можем определить гомоморфизм $\varphi : K[x]/p(x) \to L$, $\operatorname{Im}\varphi \cong K[x]/p(x)$. Понятно, что такой гомоморфизм может быть только единственным.

$\operatorname{Im}\varphi$ это алгебра и состоит из линейных комбинаций $1, \alpha, \ldots, \alpha^{n-1}$, где n – степень $p(x)$, так как он изоморфен $K[x]/p(x)$. Тогда $K[\alpha] = < 1, \alpha, \alpha^2, \ldots > = < 1, \alpha, \ldots, \alpha^{n-1} > = \operatorname{Im}\varphi$. $\operatorname{Im}\varphi$ – поле, содержащее $\alpha \Rightarrow \operatorname{Im}\varphi \supset K(\alpha) \supset K[\alpha]$, но мы уже поняли, что $K[\alpha] = \operatorname{Im}\varphi$. Отсюда

$$K[x]/p(x) \cong \operatorname{Im}\varphi = K[\alpha] = K(\alpha).$$

Пусть α не алгебраический, то есть трансцендентный. Тогда отображение $\varphi : K[x] \to L$ переводящее $x \to \alpha$ инъективно, так как $\operatorname{Ker}\varphi = \{0\}$. $\operatorname{Im}\varphi =< 1, \alpha, \ldots >$ – это $K[\alpha]$.
Далее заметим, что сущствует единственное отображение $K(x) \to L$, $\frac{f(x)}{g(x)} \to \frac{f(\alpha)}{g(\alpha)}$, потому что образы всех элементов $K[x]$, кроме 0 в L обратимы. Образ этого отображения есть подполе изоморфное $K(x)$ и имеет вид $\{\frac{f(\alpha)}{g(\alpha)}\}$. Любое поле, которое содержит α должно содержать все такие элементы. Понятно, что это и есть $K(\alpha)$. □

Следствие 5. Пусть α – алгебраическое. Тогда $\deg K[\alpha] = \deg K[x]/p(x) = \deg p(x)$, где $p(x)$ – минимальный многочлен α.

Следствие 6. Все расширения, порождённые над K корнем одного и того же неприводимого многочлена изоморфны. Часто я буду говорить, про расширение $K[\alpha]$, где α корень многочлена $p(x)$. Это корректно, так как такое расширение определено однозначно с точностью до изоморфизма.

0.38. Построение при помощи циркуля и линейки. Пример неразрешимого построения.

x – построимо $\Rightarrow$ оно алгебраическое и лежит в расширении $L/\mathbb{Q}$ степени 2^n. Докажем индукцией по числу построений, рассмотрим уравнение пересечения с новым объектом степени 2. $\cos\frac{\pi}{9}$ – корень уравнения $4x^3 - 3x = \frac{1}{2}$.

Напомню, что при построении циркулем и линейкой можно поставить пару начальных точек (задать масштаб), соединять две построенные точки прямой и строить окружность с центром в построенной точке и с расстоянием, равным расстоянию между уже построенными двумя точками. Точка построена, если она есть точка пересечения построенных прямых и окружностей.

Вещественное число x называется построимым, если стартуя с точек $(0,0)$ и $(1,0)$ можно построить отрезок $(x,0)$.

Теорема 36. Если вещественное число x построимо, то оно алгебраическое и лежит в расширении $L/\mathbb{Q}$ степени 2^m.

Доказательство. Доказательство идёт индукцией по числу построений. Пусть уже построены прямые l_i и окружности O_j. Заметим, что коэффициенты в уравнениях O_i и l_j по индукционному предположению лежат в подполе $L \subseteq \mathbb{R}$ степени 2^m над $\mathbb{Q}$. Тоже касается и новой прямой l (или окружности O). Посмотрим на пересечение окружности O_j и новой l. Она заданы уравнениями $(x-a)^2 + (y-b)^2 = r^2$ и $cx + dy = f$. Пусть $c \neq 0$. Тогда первое уравнение переписывается в виде

$$(f - dy)^2 + c^2(y-b)^2 = c^2r^2$$

Его коэффициенты из L, а решение y лежит либо в L либо в расширении степени 2 над L. Случай пересечения двух окружностей сводится к пересечению окружности и прямой. □

Следствие 7. Нельзя разбить произвольный угол на три части при помощи циркуля и линейки.

Доказательство. Например, угол $\frac{\pi}{9}$ нельзя. Действительно, построимость угла и его косинуса равносильны. Косинус $\frac{\pi}{9}$ удовлетворяет уравнению $4x^3 - 3x = \frac{1}{2}$. Это неприводимый над $\mathbb{Q}$ многочлен (так как его корни это $\cos(\alpha) : \cos(3\alpha) = \frac{1}{2}$, то есть $\alpha = \frac{\pi}{9} + \frac{2\pi k}{3}$) степени 3 и его корни не могут лежать в расширении степени 2^m. Следовательно, построение невозможно. □

0.39. Конечные поля...

Конечные поля. Число элементов. Основное уравнение. Эндоморфизм Фробениуса. Корни $x^{p^n} - x$ образуют подполе.

Хорошо смотреть на мультипл. группу. Теорема Ферма для групп. Биномиальный коэф. делится на p почти всегда.

Лемма 19. Любое поле K конечной характеристики p содержит $\mathbb{Z}/p$ как подполе

Доказательство. $\operatorname{Im} f : \mathbb{Z} \to K,\ f(x) = (x \bmod p)$ – искомое подполе. Фактически, кольцо порожденное сложением и умножением единичек. Легко проверить, что их сложение и умножение по модулю не выводит за пределы $\mathbb{Z}/p$. И $\operatorname{Im} f$ является полем, так как мы всегда умеет делить по модулю p. □

Лемма 20. Если K – конечное поле, характеристики p, то $|K| = p^n$, для некоторого n

Доказательство. Рассмотрим порядки элементов K как группы по сложению. Мы помним, что порядок элемента делит порядок группы. И обратно, для любого делителя порядка группы найдётся элемент такого порядка.

Заметим, что $\forall a \neq 0 \in K,\ (p-1)a \neq 0,\ pa = 0$. То есть нет элементов с порядком отличным от p, а значит у $|K|$ нет других делителей, кроме p. Тогда $|K| = p^n$. □

Лемма 21. Элементы $K = \mathbb{F}_{p^n}$ удовлетворяют уравнению $x^{p^n} - x = 0$

Доказательство. В K^* по теореме Ферма для групп любой элемент удовлетворяет $x^{p^n-1} = 1$, т. к. $|K^*| = p^n - 1$. Это уже всё доказывает. Осталось домножить на x, чтобы единственный элемент не из K^*, а именно 0 стал тоже удовлетворять уравнению. □

Лемма 22. Для кольца L характеристики p отображение $x \mapsto x^p$ – эндоморфизм. А если L поле, то автоморфизм. Называется эндоморфизм Фробениуса

Доказательство. Произведение, очевидно, сохраняется: $(xy)^p = x^p y^p$. Для суммы: $(x+y)^p = \sum\limits_k \binom{k}{p} x^k y^{p-k}$, но $p \mid \binom{k}{p}$, кроме $k \in \{0,\ p\}$. То есть $(x+y)^p = x^p + y^p$.

Для полей это автоморфизм, так как $x \mapsto x^{\frac{1}{p}} = x^{p^{n-1}}$ – обратный эндоморфизм. Ведь это многократный эндоморфизм Фробениуса $(x \mapsto x^p)^{\circ n-1}$. □

Лемма 23. Если L – поле характеристики p, то $K = \{x \in L\ :\ x^{p^n} = x\}$ – подполе.

Доказательство. $0, 1 \in K$. Если $x = x^{p^n},\ y = y^{p^n}$, то $xy = (xy)^{p^n}$. Если $x = x^{p^n},\ y = y^{p^n}$, то $(x+y)^{p^n} = x^{p^n} + y^{p^n}$, так как возведение в p^n – эндоморфизм (перестановочен со сложением, в частности), а именно n-кратный Фробениус. Ну и обратный к x – x^{p^n-2}, что видно из уравнения на элементы K. □

0.40. Основная теорема про конечные поля.

Теорема 37. Существует и единственно (с точностью до изоморфизма) поле из p^n элементов. Обозначается $\mathbb{F}_{p^n}$.

Поле разложения $x^{p^n} - x \to$ подполе из p^n элементов. Взять образующий группы, найти мин. многочлен, найти его корень в другом поле (через делимость). И проверить на изоморфизм "образующий группы в корень" – техника.

Доказательство теоремы. Существование. Возьмём $\mathbb{Z}/p$ и многочлен $x^{p^n} - x$ над ним. Рассмотрим такое расширение, где этот многочлен раскладывается на линейные множители. Мы знаем, что такое есть из прошлого семестра (мы умеем последовательно строить расширения, где многочлен имеет хотя бы один корень).

Рассмотрим такое поле L. В нём есть подполе элементов, удовлетворяющих $x^{p^n} - x = 0$ (по лемме). Но таких элементов ровно p^n: их не больше p^n, так как корней многочлена в поле не больше p^n, но и не меньше, так как у этого многочлена нет кратных корней (производная).

Доказательство теоремы. Единственность. Возьмём два поля K, L такие, что $|K| = |L| = p^n$.

Рассмотрим φ – образующий циклической группы K^*. Понятно тогда, что добавив φ к $\mathbb{Z}/p$ получится K, ведь φ даже умножением уже всё порождает. То есть $K \cong (\mathbb{Z}/p[x])/m_\varphi$, где m_φ – минимальный многочлен для φ.

Теперь рассмотрим m_φ над L. У него есть корни, так как $x^{p^n} - x$ делится на m_φ над обоими полями (делимость не портится при переходе между полями, ведь делимость – алгоритм Евклида, а коэффициенты вообще из базового поля).

То есть у m_φ есть корень в L – ξ, тогда $f : (\mathbb{Z}/p[x]) \to L$, $x \mapsto \xi$ – просто гомоморфизм подстановки, но он пропускается через $(\mathbb{Z}/p[x])/m_\varphi$, так как кратные m_φ уж точно зануляются. Тогда гомоморфизм $K = (\mathbb{Z}/p[x])/m_\varphi \to L$ – изоморфизм: инъективность следует из тривиальности ядра (если ядро не тривиально, то оно всё K (промежуточных нет, т. к. поля), но мы понимаем, что отображение не нулевое), сюръективность из инъективности и Дирихле.

0.41. Подполя данного конечного поля. Описание автоморфизмов...

Подполя данного конечного поля. Описание автоморфизмов F_p^n.
Необработанная версия из конспекта Константина Михайловича

Лемма 24. Пусть K — поле, $p = \operatorname{char} K$ — простое число. Тогда в K есть подполе изоморфное $\mathbb{Z}/p$. Если к тому же K — конечное, то число элементов $|K| = p^n$ для некоторого натурального n.

Доказательство. Рассмотрим гомоморфизм $f\colon \mathbb{Z} \to K$. Ядро этого отображения это $p\mathbb{Z}$. Тогда $\operatorname{Im} f \cong \mathbb{Z}/p$. Пусть теперь K конечно. Рассмотрим K как группу по сложению. Заметим, что порядок любого ненулевого элемента равен p. Так как нет элементов другого порядка, то в группе p^n элементов по теореме Коши. □

Обычно доказательство идёт через линейную алгебру.

Теорема 38. Существует и единственно (с точностью до изоморфизма) поле из p^n элементов. Такое поле будем обозначать $\mathbb{F}_{p^n}$.

Начнём с леммы:

Лемма 25. Пусть K поле из p^n элементов. Тогда все элементы K удовлетворяют уравнению $x^{p^n} = x$.

Доказательство. Группа K^* состоит из $p^n - 1$ элементов. Тогда все элементы из K^* удовлетворяют уравнению $x^{p^n-1} - 1 = 0$. Домножая на x добавляем неприкаянный 0. □

Лемма 26. Пусть L — кольцо характеристики p. Тогда отображение $x \to x^p$ является эндоморфизмом L. Это отображение называется эндоморфизмом Фробениуса. Если L - конечное поле, то эндоморфизм Фробениуса является автоморфизмом.

Доказательство. Очевидно произведение переходит в произведение. $(x+y)^p = \sum_{i+j=p} \binom{p}{i} x^i y^j = x^p + y^p$ т.к. все промежуточные биномиальные коэффициенты делятся на p. Пусть теперь L – поле. Тогда заметим, что отображение Frob инъективно, так как в поле не бывает нильпотентов и, следовательно, по принципу Дирихле, биективно. □

Лемма 27. Пусть L — поле характеристики p. Тогда множество элементов из L удовлетворяющих уравнению $x^{p^n} = x$ образует подполе в L.

Доказательство. Обозначим рассматриваемое множество за K. Тогда $0, 1 \in K$. Очевидно, что K замкнуто относительно умножения. Замкнутость относительно сложения следует из того, что x^{p^n} есть композиция n раз эндоморфизма Фробениуса. Значит K — подкольцо. Обратный к $x \neq 0$ имеет вид x^{p^n-2}, что следует из уравнения. □

Доказательство теоремы. Существование. Рассмотрим поле $\mathbb{F}_p = \mathbb{Z}/p$ и $x^{p^n} - x$ — многочлен над ним. Тогда есть поле L в котором $x^{p^n} - x$ раскладывается на линейные множители. Рассмотрим K — подполе в L состоящее из элементов удовлетворяющих уравнению $x^{p^n} = x$. В K ровно p^n элементов т.к. многочлен $x^{p^n} - x$ не имеет кратных корней.

Доказательство теоремы. Единственность. Пусть есть два поля K и L из p^n элементов. Рассмотрим их мультипликативные группы. Они циклические порядка $p^n - 1$. Пусть группа K^* порождена элементом ξ. Тогда любой элемент заведомо является многочленом от ξ. Пусть f – минимальный многочлен ξ. Значит $K \cong \mathbb{F}_p[x]/f(x)$. Многочлен f неприводим. ξ — его корень. Многочлен $x^{p^n} - x$ делится на f, так как у них есть общий корень ξ. Тогда у f есть корни в любом поле из p^n элементов, в частности в L. Тогда у нас есть гомоморфизм $K \cong \mathbb{F}_p[x]/f(x) \to L$ переводящий ξ в какой-то корень f. Этот гомоморфизм инъективен и по принципу Дирихле является биекцией. □

Замечание. В частности, мы увидели, что любое конечное поле $\mathbb{F}_{p^n}$ имеет вид $K \cong \mathbb{F}_p[x]/f(x)$. Степень f равна n исходя их подсчёта числа элементов.

Теорема 39. Поле $\mathbb{F}_{p^n}$ подполе $\mathbb{F}_{p^m}$ тогда и только тогда, когда $m \vdots n$. Такое подполе единственно.

Доказательство. Если $\mathbb{F}_{p^n}$ подполе $\mathbb{F}_{p^m}$, то сравнивая степени расширения получаем, что $m \vdots n$. Обратно, возьмём в $\mathbb{F}_{p^m}$ подполе $\{x \in \mathbb{F}_{p^m} \mid x^{p^n} - x = 0\}$. Очевидно, что любое подполе из p^n элементов там содержится. Это даёт единственность. Для того, чтобы доказать существование покажем, что в указанном подполе p^m элементов. Для этого заметим, что многочлен $x^{p^m} - x \vdots x^{p^n} - x$, если $m \vdots n$. Первый многочлен раскладывается на линейные множители над $\mathbb{F}_p$, откуда аналогичное свойство выполнено для второго многочлена. То есть у многочлена $x^{p^n} - x$ есть все p^n корней в $\mathbb{F}_{p^m}$. Что и требовалось. □

Покажем, что аналогичные свойства верны для расширений поля $\mathbb{F}_q$, где $q = p^n$. Большая их часть, естественно, сводится к расширениям $\mathbb{F}_p$, однако, в некоторых вопросах возникают дополнительные сложности. Основная из них – наличие нетривиальных автоморфизмов у таких полей над $\mathbb{F}_p$. Начнём с леммы.

Лемма 28. Все автоморфизмы $\mathbb{F}_q$ над $\mathbb{F}_p$ имеют вид $\mathrm{Frob}_p^{\circ i}$, где $0 \le i \le n-1$.

Доказательство. Заметим, что поле $\mathbb{F}_q$ порождено одним элементом $\mathbb{F}_q = \mathbb{F}_p[\alpha]$. Минимальный многочлен α над $\mathbb{F}_p$ обозначим за f, его степень равна n.

Теперь, гомоморфизмы $\mathbb{F}_p[\alpha]$ определяются образами элемента α, которые обязаны быть корнями того же многочлена f. Но таких корней в $\mathbb{F}_p[\alpha]$ не более n. Тогда и автоморфизмов не более n! Осталось показать, что мы нашли все n возможных. Для этого предположим, что для всех элементов из $\mathbb{F}_q$ выполнено, что $\mathrm{Frob}_p^{\circ l} - \mathrm{Frob}_p^{\circ k} = 0$, для $k, l < n$. Но это уравнение степени меньше p^n. Ему не могут удовлетворять все элементы $\mathbb{F}_q$! □

0.42. Расширения поля, неприводимые многочлены...

Расширения поля F_q . Неприводимые многочлены как делители $x^{q^d} - x$.
Необработанная версия из конспекта Константина Михайловича

Теорема 40. Все расширения поля $\mathbb{F}_q$, где $q = p^n$ имеют q^m элементов. Два расширения $\mathbb{F}_q$ из q^m элементов изоморфны между собой. Внутри поля $\mathbb{F}_{q^m}$ есть подполе $\mathbb{F}_{q^l}$ только если $l|m$.

Доказательство. Если L расширение $\mathbb{F}_q$, то оно имеет $q^{[L:\mathbb{F}_q]}$ элементов. Покажем существование. Возьмём поле из $q^m = p^{nm}$ элементов и рассмотрим в нём подполе $\mathbb{F}_q$ из $q = p^n$ элементов. Такое есть по предыдущей теореме. Это и даёт необходимое расширение.

Покажем единственность такого расширения с точностью до $\mathbb{F}_q$ изоморфизма. Основная сложность состоит в том, чтобы проследить за сохранением $\mathbb{F}_q$ коэффициентов. Итак, пусть L_1 и L_2 – расширения $\mathbb{F}_q$ из q^m элементов. Такие поля изоморфны над $\mathbb{F}_p$. Пусть $\varphi\colon L_1 \to L_2$ изоморфизм над $\mathbb{F}_p$. Вообще говоря он не обязан переводить элементы из $\mathbb{F}_q$ в себя же. Нам надо подправить его, чтобы он так делал. Для этого заметим, что $\varphi(\mathbb{F}_q) = \mathbb{F}_q$. Таким образом у нас возникает автоморфизм $\mathbb{F}_q \to \mathbb{F}_q$. Он имеет вид $\mathrm{Frob}^{\circ i}$. Тогда на всём поле L_2 рассмотрим автоморфизм $\varphi' = \mathrm{Frob}^{\circ -i}$. Тогда композиция $\varphi' \circ \varphi$ и есть подходящий изоморфизм.

Теперь рассмотрим поле из q^m элементов. Тогда в нём есть подполе из q^l элементов только если $nm \vdots nl$. Но это происходит только если $m \vdots l$. Такое подполе единственно и автоматически снабжается структурой $\mathbb{F}_q$ расширения, так как содержит образ последнего при его вложении в $\mathbb{F}_{q^m}$. □

Покажем одну полезную теорему про многочлены над конечным полем.

Теорема 41. Пусть $f(x)$ – это неприводимый многочлен из $\mathbb{F}_q[x]$. Тогда $x^{q^m} - x \vdots f(x)$ тогда и только тогда, когда $\deg f(x)|m$.

Доказательство. Пусть $x^{q^m} - x$ делится на $f(x)$. Тогда в поле $\mathbb{F}_q^m$ многочлен $f(x)$ имеет корень α (на самом деле там лежат все его корни). Теперь $\mathbb{F}_q[\alpha]$ подполе $\mathbb{F}_{q^m}$. Но тогда $\deg f(x) = [\mathbb{F}_q[\alpha] : \mathbb{F}_q] \vdots m$.

Обратно, пусть $k = \deg f(x)|m$. Тогда в $\mathbb{F}_q^m$ есть подполе $\mathbb{F}_{q^k}$. Но такое подполе изоморфно $\mathbb{F}_q[x]/f$ и имеет внутри корень α многочлена $f(x)$. Но тогда $f(x)$ и $x^{q^m} - x$ не взаимно просты, откуда следует, что $x^{q^m} - x \vdots f(x)$, благодаря неприводимости последнего. □

0.43. Лемма про производную. Лемма про корень...

Лемма про производную. Лемма про эффективное извлечение корня степени p.
Необработанная версия из конспекта Константина Михайловича

Я опишу здесь некоторый набор соображений и алгоритмов касательно разложения многочленов на множители над конечным полем.

Мы помним, что над полями характеристики 0 всегда легко выделить все кратные множители многочлена просто взяв отношение f и НОД(f, f'). Однако, над конечными полями всё немного не так. Точнее

Лемма 29. Пусть $f = \prod g_i^{n_i}$. Тогда

$$\text{НОД}(f, f') = \prod_{n_i \nvdots p} g_i^{n_i - 1} \prod_{n_i \vdots p} g_i^{n_i}.$$

Доказательство. Рассмотрим неприводимый множитель g_i. Пусть $f(x) = g_i(x)^{n_i} g(x)$. Продифференцируем. Имеем $f'(x) = n_i g_i'(x) g_i^{n_i - 1} + g_i^{n_i} g'(x)$. Если $n_i \nvdots p$, то кратность вхождения $g_i(x)$ в $f'(x)$ равна $n_i - 1$. Если же $n_i \vdots p$, то $f'(x) = g_i^{n_i} g'(x)$, что показывает, что степень вхождения g_i в НОД(f, f') не менее n_i. Но степень вхождения g_i в $f(x)$ ровно n_i. Откуда степень вхождения g_i в НОД n_i, что и требовалось.

Лемма 30. Многочлен h над конечным полем характеристики p имеет нулевую производную тогда и только тогда, когда он является p-ой степенью. Извлечение степени можно провести эффективно.

Доказательство. Как мы уже знаем с прошлого семестра, если $h' = 0$, то $h = g(x^p)$. Посмотрим на коэффициенты $g - a_0, \ldots, a_l \in \mathbb{F}_q$. Вспомним, что эндоморфизм Фробениуса Frob: $\mathbb{F}_q \to \mathbb{F}_q$ – биекция. Иными словами из каждого элемента можно извлечь корень степени p. Пусть $b_i^p = a_i$. Тогда $f = b_0 + b_1 x + \cdots + b_l x^l$ обладает свойством $f^p = g(x^p) = h$. Как вычислить корень степени p из элемента? Для этого заметим, что обратное отображение к Frob: $\mathbb{F}_q \to \mathbb{F}_q$ это $\text{Frob}^{\circ n-1}$. □

0.44. Лемма про разделение на сомножители, чьи неприводимые множители имеют одинаковую степень.

Необработанная версия из конспекта Константина Михайловича

Это позволяет свести задачу разложения произвольного многочена над конечным полем к разложению на множители многочлена без кратных множителей. Действительно $\frac{f}{\text{НОД}(f,f')}$ без кратных множителей. В свою очередь НОД(f, f') состоит из множителей двух типов – чьи степени кратны p и не кратны p. Первые встречаются как сомножители в $\frac{f}{\text{НОД}(f,f')}$ и легко находятся после получения его разложения. Из оставшихся множителей можно извлечь корень степени p и перейти к разложению многочлена заведомо меньшей степени.

Другое соображение позволяет свести задачу к разложению многочленов, чьи неприводимые сомножители имеют одинаковую степень.

Заметим, что неприводимый многочлен степени k, является делителем $x^{q^k} - x$, но не являются делителями $x^{q^l} - x$ ни для каких $l < k$. Пусть f – многочлен степени ровно n над $\mathbb{F}_q$. Без ограничения общности будем считать, что многочлен f без квадратов.

Теорема 42. Существует полиномиальная от размера f (то есть от $n \log q$) процедура, которая разделяет f на сомножители $f_1, \ldots, f_k$, что f_i состоит из неприводимых сомножителей степени ровно i.

Доказательство. Переберём все многочлены вида $g_l = x^{q^l} - x$, где $l < n$. Пусть на шаге l у многочлена f нет неприводимых множителей степени меньше l. Тогда НОД(g_l, f) состоит из всех множителей степени ровно l (они ведь входят в f с кратностью 1). Тогда $\frac{f}{\text{НОД}(g_l,f)}$ состоит из неприводимых множителей степени больше l

Осталось пояснить, как посчитать НОД(f, g_l). Проблема в том, что размер g_l не полиномиально зависит от размера f. Здесь на помощь приходит следующее соображение: пусть r – остаток от деления g_l на f. Тогда НОД$(g_l, f) =$ НОД(r, f). Степень же r меньше степени f. Осталось понять, как быстро найти r. Для этого надо вычислить $x^{q^l} \bmod f$. Но для этого надо всего лишь возвести x в степень q^l в кольце $\mathbb{F}_q[x]/f$, что делается за $l \log q$ операций умножения в этом кольце, то есть за $l \log q$ умножений многочленов степени меньше n и вычислений остатков для многочленов степени не более $2n$. □

0.45. Алгоритм Берлекэмпа.

Теорема 43 (Алгоритмы Берлекэмпа)**.** Пусть $f(x) \in \mathbb{F}_q$ без кратных множителей. Тогда существуют детерминированный полиномиальный по n (но не по $\log q$) алгоритм раскладывающий f на множители.

Доказательство. Первое соображение, которое мы применим, будет состоять в том, что мы переформулируем задачу факторизации многочлена f как задачу про некоторое кольцо. Точнее, пусть $f = h_1 \ldots h_l$ разложение на неприводимые. Тогда по Китайской теореме об остатках

$$R = \mathbb{F}_q[x]/f \cong \mathbb{F}_q[x]/h_1 \times \cdots \times \mathbb{F}_q[x]/h_l.$$

Заметим, что нахождение нетривиального делителя нуля в R равносильно нахождению делителя f. Заметим, что, в свою очередь, $\mathbb{F}_q[x]/h_i$ – поле из $q^{\deg h_i}$ элементов. Делителем нуля является любой элемент с хотя бы одним нулём в компоненте.

В каждом таком поле есть единственное подполе из q элементов, состоящее из решений уравнения $x^q - x = 0$. Если рассмотреть множество решений этого уравнения в R, то оно будет состоять из l-ек покомпонентных решений. Иными словами множество решений уравнения $x^q - x$ в R есть подалгебра R', изоморфная $\mathbb{F}_q \times \cdots \times \mathbb{F}_q$, взятое l раз. Если мы найдём делитель нуля в этой подалгебре, то найдём и в исходной. Заметим, что удельно, делителей нуля в этой подалгебре больше чем в исходной.

Как найти R'? Для этого надо найти все решения уравнения $x^q - x = 0$ в R. Второе соображение состоит в том, что это уравнение линейно (над $\mathbb{F}_q$). Чтобы решить это линейное уравнение надо составить его матрицу. У отображения $x \to -x$ матрица $-E_n$, где $n = \deg f$. У оператора $x \to x^q$ матрица легко считается. Далее достаточно применить любой из методов для решения систем линейных уравнений. Заметим, что если алгебра R' одномерна (она не менее чем одномерна, так как константа всегда решение), то многочлен f неприводим.

Теперь мы нашли R'. Построим детерминированный алгоритм нахождения разложения. Напомню, что нам надо получить делитель нуля, то есть элемент, у которого хоть одна компонента не 0. Возьмём произвольный не константный элемент h из R'. Тогда h соответствует l-ка $(a_1, \ldots, a_l)$. Переберём все константы c из $\mathbb{F}_q$. Их q штук (это и даёт неполиномиальность алгоритма по $\log q$). Тогда $h - c$ для, например, $c = a_1$ есть нетривиальный делитель 0 (он не ноль, потому что h не константа).

Делитель f теперь можно найти как НОД$(f, h - c)$.

□

0.46. Вероятностный алгоритм Кантора-Цассенхауза.

Теорема 44 (Алгоритмы Кантора-Цассенхауза)**.** Пусть $f(x) \in \mathbb{F}_q$ без кратных множителей, $q \neq 2^d$. Тогда существуют вероятностный полиномиальный по $n \log q$ алгоритм раскладывающий f на множители.

Доказательство. Будем предполагать, что $f(x)$ имеет в качестве неприводимых делителей многочлены степени ровно d. Тогда алгебра R имеет вид

$$R = \mathbb{F}_q[x]/f(x) \cong \mathbb{F}_{q^d} \times \cdots \times \mathbb{F}_{q^d}.$$

Для упрощения обозначений я заменю q^d на l. Посмотрим отдельно на один сомножитель $\mathbb{F}_l$. Заметим, что любой элемент поля $\mathbb{F}_l$ удовлетворяет условию, что $x^{\frac{l-1}{2}}$ либо 0, либо 1, либо -1. Ноль реализуется только в случае $x = 0$, а 1 и -1, если x квадрат и не квадрат соответственно. Из этого стоит пояснить, что, если x не квадрат, то $x^{\frac{l-1}{2}}$ элемент порядка 2 (и следовательно равен -1). Действительно, любой элемент $\mathbb{F}_l^*$ есть степень некоторого элемента α. Тогда элемент квадрат только если он есть α^{2d}. В свою очередь, элемент α^{2d+1} не может быть тривиальным, потому что порядок α чётен. В частности $(\alpha^{2k+1})^{\frac{q-1}{2}}$ с одной стороны имеет порядок либо 2, либо 1 и при этом не тривиален, то есть порядка 2.

Возьмём теперь случайный элемент из алгебры R, при условии, что все неприводимые множители f одной степени, скажем d. В последнем случае вся алгебра

$$R \cong \mathbb{F}_{q^d} \times \cdots \times \mathbb{F}_{q^d}$$

есть произведение одинаковых полей. Наша задача придумать вероятностный алгоритм находящий делитель нуля в таком произведении. Для этого возьмём случайный элемент a из R. Если a делитель нуля всё и так хорошо. Это можно проверить взяв НОД(f, a), который заодно вычислит делитель f. Иначе с вероятностью больше чем $\frac{1}{2}$ одна из компонент a является квадратом, а ещё одна не является квадратом. Пусть это первая или вторая компоненты. Тогда $a^{\frac{q-1}{2}}$ имеет вид $(1, -1, \ldots)$ и $a - 1$ является нетривиальным делителем нуля. □

0.47. След, его нетривиальность. Алгоритм...

След, его нетривиальность. Ещё один алгоритм разложения для $q = 2$.

Осталось единственное «Но». Это не работает в характеристике 2. В случае характеристики 2 рассмотрим следующее выражение:

$$U(y) = y + y^q + \cdots + y^{q^{d-1}}.$$

Это линейное отображение $\mathbb{F}_{q^d} \times \cdots \times \mathbb{F}_{q^d} \to \mathbb{F}_q \times \cdots \times \mathbb{F}_q$ лежащее внутри R. Я утверждаю, что это отображение невырождено. Для этого проверим это свойство для отображения $\mathbb{F}_{q^d} \to \mathbb{F}_q$. Для этого заметим, что $U(x)$ есть многочлен степени q^{d-1} и, следовательно, не может иметь более q^{d-1} корней. Это означает, что его ядро есть не всё $\mathbb{F}_{q^d}$, откуда получаем требуемое.

Пусть $q = 2$. Возьмём теперь степени образующей $1, x, \ldots, x^{2d-1}$. По китайской теореме об остатках существует такой многочлен $p(x)$, что $\deg p(x) < 2d$ и остаток $U(p(x))$ по модулю f_1 равен 0 и по модулю f_2 равен 1. Но тогда есть и для некоторого l x^l обладает свойством, что $U(x^l)$ имеет разные остатки по модулю f_1 и f_2. Но тогда, один из этих остатков 0, а ещё один единица. Отсюда получаем, что $U(x^l)$ – даёт нетривиальный делитель нуля в R.

Замечание. Есть алгоритм, позволяющий свести разложение многочлена над $\mathbb{F}_{q^d}$ к разложению многочлена над $\mathbb{F}_q$.

0.48. Коды, исправляющие ошибки...

Коды, исправляющие ошибки. Минимальное расстояние. Линейные коды. Вычисление минимального расстояния для линейных кодов.

Шпаргалка: да вроде и не нужна?

Сообщения – это строки длины n из алфавита $\mathcal{A}$. Хотим их кодировать – сопоставить каждой строке из $\mathcal{A}^n$ строку из $\mathcal{B}^m$ так, чтобы даже если сообщение немного поломается при передаче можно было понять, что передавали.

Считаем, что единственные проблемы, случающиеся со строками при передаче это изменение в нескольких позициях.

Определение (Расстояние Хемминга)**.** Пусть даны два слова $x, y \in \mathcal{A}^n$. Тогда расстоянием Хемминга между ними называется число позиций, в которых эти слова различаются

$$\rho_H(x, y) = |\{1 \le i \le n \,|\, x_i \ne y_i\}|.$$

Хотим, чтобы наши коды были устойчивы к таким изменениям.

Определение. Кодом называется подмножество $C \subseteq \mathcal{B}^m$ равномощное $\mathcal{A}^n$. Его элементы называются кодовыми словами.

Определение. Кодовым расстоянием называется величина

$$d_{min} = \min_{\substack{x,y \in C \\ x \ne y}} \rho_H(x, y).$$

Определение. Код C обнаруживает d ошибок, если ни в каком кодовом слове нельзя сделав $\le d$ ошибок получить другое кодовое слово. Эквивалентно тому, что $\forall x, y \in C \ \rho_H(x, y) > d$, эквивалентно $d_{min} > d$

Определение. Будем исправлять ошибки максимально просто – приняв какую-то строку возьмем ближайшее по расстоянию Хэмминга кодовое слово. Код C исправляет d ошибок, если при исправлении любого кодового слова, дошедшего с $\le d$ ошибками, получается исходное слово. То есть на расстоянии d от кодового слова ближайшим будет оно само, то есть расстояние до остальных будет больше, то есть расстояние от кодового слова до остальных хотя бы $2d + 1$ то есть $d_{min} \ge 2d + 1$.

Обычно алфавиты исходных строк и кодов выбирают одинаковыми. Будем обозначать размер алфавита за q. Если $q = 2$ то коды называются бинарными.

Особенно удобно и алгебраично работать с алфавитами размера $q = p^n$, считать что на нем задано конечно поле, и искать линейные отображения $K \colon \mathbb{F}_q^k \to \mathbb{F}_q^n$

Определение. Линейным n, k, q-кодом называется k-мерное подпространство в $\mathbb{F}_q^n$. Отношение $\frac{k}{n}$ называется скоростью кода.

Если отображение K линейно, то оно задаётся матрицей размера $n \times k$ и ранга k (инъекция), которая обозначается G и называется порождающей матрицей. Одному коду могут соответствовать разные K.

Определение. Кодирование называется систематическим, если G имеет вид $(E_k|G')$. Такая матрица гарантирует, что первые k знаков исходного сообщения записаны в первые k знаков исходного слова, следовательно проще декодировать если нет ошибок.

Определение. C – подпространство, значит есть H – матрица $n - k \times n$ ранга $n - k$, что $\operatorname{Ker} H = C$. Такая матрица называется проверочной матрицей кода C. $\operatorname{Ker} H = \operatorname{Im} G \Rightarrow HG = 0$

Часто проверочной матрицей называют матрицу $H^\top$. Это удобно, если заметить, что такая матрица является порождающей $(n, n - k, q)$ кода (т.к. ее ранг $n - k$). Почему удобно – загадка (TODO)

Лемма 31. Пусть C – линейный код. Тогда кодовое расстояние d равно

$$d = \min_{\substack{x \in C \\ x \ne 0}} \rho_H(0, x) =$$

мин кол-во линейно зависимых столбцов H.

Доказательство.

$$\rho_H(x, y) = \rho_H(x - y, 0) \Rightarrow \min \rho_H(x, y) = \min \rho_H(x, 0)$$

$x \in C \Leftrightarrow Hx = 0$. Минимальное кол-во отличных от нуля значений в x очевидно равно мин кол-во линейно зависимых столбцов H. □

Как декодировать полученное сообщение? Пусть v – то, что пришло, $Hv = s$. Надо найти $w \in C = \operatorname{Im} G$, что $v - w$ минимально отличается от 0 (по ρ_H). Можно перебрать все $u \in \mathbb{F}_q^k$ и выбрать ближайший к 0 из $v - Gu$. Но это долговато. Для лучшего результата понадобятся циклический коды, но это уже совершенно другой вопрос.

0.49. Циклические коды. Эквивалентное описание. Коды БЧХ. Пример.

Шпаргалка: $q = p^s$, m, n такие, что $q^m - 1 \vdots n$, $2 \le d \le n$, $l_0 \le n$. α – образующая ${\mathbb{F}_{q^m}}^*$, $\beta = \alpha^{(q^m-1)/n}$

Будем смотреть на множество слов $\mathbb{F}_q^n$ как на $\mathbb{F}_q[x]/x^n - 1$ и рассматривать коды только вида $I \le \mathbb{F}_q[x]/x^n - 1$, гд I – идеал.

Теорема 45. Пусть $C \le \mathbb{F}_q[x]/x^n - 1$ подпространство. Тогда C идеал тогда и только тогда, когда для всякого слова $(a_0, \dots, a_{n-1}) \in C$ слово $(a_{n-1}, a_0, \dots, a_{n-2})$ тоже из C.

Доказательство. Достаточно чтобы домножение на x оставляло любой элемент I в I. Т.к. $x^n = 1$, домножение на x это циклический сдвиг. □

Определение. Такие коды называются циклическими.

Идеалы в этом кольце однозначно сопоставляются делителям $x^n - 1$ (т.к. взаимно простые с нем многочлены обратимы). Каждый делитель $g \vdots x^n - 1$ степени $\deg g = l$ дает нам $n, n-l, q$ код ($n - l$ т.к. $\frac{x^n-1}{g}$ – минимальный, переводимый в ноль домножением на g).

Кодировать можно разными способами. Самое простое – тупо домножить. Но можно сделать систематическое кодирование

$$m(x) \to m(x)x^l - r(x), \text{ где } r(x) = x^l m(x) \bmod g(x).$$

Здесь строго говоря $m(x)$ записан в последние биты.

Определение. Коды БЧХ. Выберем $q = p^s$, m, n такие, что $q^m - 1 \vdots n$, $2 \le d \le n$, $l_0 \le n$. α – образующая ${\mathbb{F}_{q^m}}^*$, $\beta = \alpha^{(q^m-1)/n}$. d называется конструктивным расстоянием. Спойлер – оно не меньше кодового расстояния.

Рассмотрим элементы $\beta^{l_0}, \beta^{l_0+1}, \dots, \beta^{l_0+d-2}$ и многочлен наименьшей степени $g(x)$, корнями которого являются эти элементы.

$\beta^n - 1 = \alpha^{q^m-1} - 1 = 1 - 1 = 0$ поэтому $x^n - 1$ от степеней β равен 0, значит $x^n - 1$ делится на g.

(мб описание проверочной матрицы входит в этот билет. Я ее вставил в следующий)

Пример тупо из конспекта:
Пусть $q = 2$. Возьмём $n = 2^4 - 1 = 15$ (то есть $m = 4$). Для того, чтобы построить поле из 16 элементов рассмотрим многочлен x^4+x^3+1. Он неприводим над $\mathbb{F}_2$. Его корень α – первообразный корень степени 15 из единицы. Возьмём $l_0 = 1$ и $d = 5$. Тогда необходимо найти минимальные многочлены для элементов $\alpha, \alpha^2, \alpha^3, \alpha^4$. Заметим, что минимальные многочлены для $\alpha, \alpha^2, \alpha^4$ одинаковы и равны $x^4 + x^3 + 1$ так как два последних элемента есть образы предыдущих при автоморфизме Фробениуса. Минимальный многочлен для α^3 равен $x^4 + x^3 + x^2 + x + 1$.

0.50. Основная теорема про коды БЧХ.

Шпаргалка: Делится $\Leftrightarrow$ обнуляется на корнях. Пусть плохо $\mathbb{F}_q$, тогда плохо в $\mathbb{F}_{q^m}$, определитель.

Определение. Коды БЧХ. Выберем $q = p^s$, m, n такие, что $q^m - 1 \vdots n$, $2 \le d \le n$, $l_0 \le n$. α – образующая ${\mathbb{F}_{q^m}}^*$, $\beta = \alpha^{(q^m-1)/n}$.

Проверочная матрица для БЧХ-кода.
Заметим, что для $f(x) \in \mathbb{F}_q[x]$ верно, что $f(x) \vdots g(x)$ тогда и только тогда, когда $f(\beta^i) = 0$ для $i \in \overline{l_0, l_0 + d - 2}$. Это приводит к следующей матрице H:

$$H = \begin{pmatrix} 1 & \beta^{l_0} & \dots & \beta^{l_0(n-1)} \\ \vdots & & \dots & \vdots \\ 1 & \beta^{l_0+d-2} & \dots & \beta^{(l_0+d-2)(n-1)} \end{pmatrix}.$$

Это матрица не над $\mathbb{F}_q$, а над $\mathbb{F}_{q^m}$. Впрочем, легко сделать из неё матрицу над $\mathbb{F}_q$ расписав все по базису. (Тогда β^i заменятся на квадратики $m \times m$)

Теорема 46. Основная теорема: Для БЧХ-кода минимальное расстояние больше или равно конструктивного.

Доказательство. Пусть есть какой-то вектор над $\mathbb{F}_q$, отличный от нуля в $< d$ позициях, который обнуляется H. Рассмотрим его как вектор в $\mathbb{F}_{q^m}$. Он все еще обнуляет H (версию в поле F_{q^m}) и все еще отличается от 0 в $< d$

позициях $\Rightarrow$ есть $d-1$ линейно зависимых столбцов.
Возьмём столбцы с номерами $i_1, \dots, i_{d-1}$. Получим матрицу

$$\begin{pmatrix} \beta^{l_0 i_1} & \dots & \beta^{l_0 i_d} \\ \vdots & & \vdots \\ \beta^{(l_0+d-2)i_1} & \dots & \beta^{(l_0+d-2)i_d} \end{pmatrix}.$$

Посчитаем её определитель. Из j-го столбца вынесем $\beta^{l_0 i_j}$. Имеем

$$\det \begin{pmatrix} \beta^{l_0 i_1} & \dots & \beta^{l_0 i_{d-1}} \\ \vdots & & \vdots \\ \beta^{(l_0+d-2)i_1} & \dots & \beta^{(l_0+d-2)i_{d-1}} \end{pmatrix} = \beta^{l_0(i_1+\dots+i_{d-1})} \det \begin{pmatrix} 1 & \dots & 1 \\ \vdots & & \vdots \\ \beta^{(d-2)i_1} & \dots & \beta^{(d-2)i_{d-1}} \end{pmatrix}.$$

Но определитель последней матрицы есть определитель Вандермонда для элементов $\beta^{i_1}, \dots, \beta^{i_{d-1}}$. Этот определитель не обращается в ноль так как $\beta^{i_k} \neq \beta^{i_l}$, если $k \neq l$.

□

0.51. Алгоритм декодирования Питерсона-Горенштейна-Цирлера.

Пример:
Пусть $q = 2$. Возьмём $n = 2^4 - 1 = 15$ (то есть $m = 4$). Для того, чтобы построить поле из 16 элементов рассмотрим многочлен x^4+x^3+1. Он неприводим над $\mathbb{F}_2$. Его корень α – первообразный корень степени 15 из единицы. Возьмём $l_0 = 1$ и $d = 5$. Тогда необходимо найти минимальные многочлены для элементов $\alpha, \alpha^2, \alpha^3, \alpha^4$. Заметим, что минимальные многочлены для $\alpha, \alpha^2, \alpha^4$ одинаковы и равны $x^4 + x^3 + 1$ так как два последних элемента есть образы предыдущих при автоморфизме Фробениуса. Минимальный многочлен для α^3 равен $x^4 + x^3 + x^2 + x + 1$.

В качестве многочлена задающего код БЧХ с конструктивным расстоянием 5 можно взять

$$g(x) = (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1).$$

Упражнение 2. *Постройте проверочную матрицу для этого кода.*

Опишем простейший алгоритм декодирования – алгоритм Питерсона-Горенштейна-Цирлера.

Пусть на вход мы получили многочлен $v(x) = u(x) + e(x)$, где $u(x)$ – это пересылаемое сообщение, а $e(x)$ – ошибка. Предположим, что $e(x) = e_{i_1}x^{i_1} + \dots + e_{i_t}x^{i_t}$ состоит из не более чем t мономов, где $t < \frac{d}{2}$, то есть мы можем раскодировать сообщение. В этом случае $2t < d$. Для того чтобы узнать, что ошибки есть, мы вычисляем $v(\beta^i)$, где $i \in \overline{l_0, l_0 + d - 2}$. Но так как $u(x) \vdots g(x)$, то

$$v(\beta^i) = u(\beta^i) + e(\beta^i) = e(\beta^i).$$

Итого мы знаем значения $e(\beta^i)$. Обозначим за

$$S_k = e(\beta^{l_0+k-1}),\ X_k = \beta^{l_0+k-1} \text{ и } Y_k = e_{i_k}.$$

В этих обозначениях S_k перепишется как

$$S_k = \sum_{i=1}^{t} Y_i X_i^{l_0+k-1}.$$

Если известны X_k, то из указанных выше уравнений легко найти y_k. Определитель матрицы этой системы есть, как и в доказательстве теоремы, определитель Вандермонда.

Итого, необходимо найти элементы X_k. Уравнения на X_k не линейны. Наша задача ввести новые величины, однозначно определяющие X_k, на которые уже можно написать линейные уравнения. Для этого рассмотрим многочлен

$$\Lambda(x) = (1 - xX_1) \dots (1 - xX_t) = 1 + \Lambda_1 x + \dots + \Lambda_t x^t.$$

Корни этого уравнения – это величины $X_1^{-1}, \dots, X_t^{-1}$. Если мы найдём Λ_i, то сможем найти X_i^{-1} и, следовательно, найти X_i. Напишем тождество

$$0 = \Lambda(X_l^{-1}) = 1 + \Lambda_1 X^l + \dots + \Lambda_t X_l^{-t}.$$

Домножим его на $Y_l X_l^{\nu+t}$ и просуммируем по l. Имеем

$$0 = \sum_{l=1}^{t} Y_l X_l^{\nu+t} + \sum_{l=1}^{t} \Lambda_1 Y_l X_l^{\nu+t+1} + \dots + \sum_{l=1}^{t} \Lambda_t Y_l X_l^{\nu}.$$

Теперь, коэффициенты при Λ_i есть некоторые известные S_k. Если взять $\nu \in \overline{l_0, l_0 + t - 1}$, то получим следующую систему уравнений

$$\begin{cases} -S_{t+1} &= \Lambda_t S_1 + \cdots + \Lambda_1 S_t \\ &\vdots \\ -S_{2t} &= \Lambda_t S_t + \cdots + \Lambda_1 S_{2t} \end{cases}$$

Разрешимость этой системы зависит от её матрицы, которая имеет вид

$$\Sigma = \begin{pmatrix} S_1 & \dots & S_t \\ \vdots & & \vdots \\ S_t & \dots & S_{2t} \end{pmatrix}.$$

Осталось заметить, что

$$\begin{pmatrix} S_1 & \dots & S_t \\ \vdots & & \vdots \\ S_t & \dots & S_{2t} \end{pmatrix} = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & & \vdots \\ X_1^{t-1} & \dots & X_t^{t-1} \end{pmatrix} \begin{pmatrix} Y_1 X_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & Y_t X_t \end{pmatrix} \begin{pmatrix} 1 & \dots & X_1^{t-1} \\ \vdots & & \vdots \\ 1 & \dots & X_t^{t-1} \end{pmatrix}.$$

Теперь, если ошибок было меньше чем t, то определитель этой матрицы 0 так как ранг средней матрицы меньше n. Если же ошибок ровно t, то определитель матрицы не ноль.

Итого мы получаем следующий алгоритм

1) Запускаем цикл по t от 1 до $\frac{d}{2}$. Вычисляем $S_1, \dots, S_{2t}$ и смотрим на определитель матрицы Σ. Если он ноль, то переходим к $t+1$. Если он не ноль, то решаем систему и находим Λ_i.

2) По Λ_i находим X_l^{-1} после чего находим позиции i_l. Это можно сделать подставив все возможные β^i в $\Lambda(x)$. Если получился корень, то надо взять $-i \bmod n$.

3) Далее, решив систему линейных уравнений можно найти e_{i_l}. Осталось вычесть и найти $u(x) = v(x) - e(x)$.

0.52. Арифметические функции...

Примеры. Функции Дирихле. Свёртка Дирихле и её кольцевые свойства. Мультипликативные функции. Примеры.

В теории чисел часто встречаются функции от натурального параметра n, которые выдают некоторое число, которое как-то завязано на свойствах кольца $\mathbb{Z}/n$. Это несколько загадочная часть теории чисел. Эта область выглядит скорее как техническое средство. Тем не менее обходить её стороной не стоит. Основной тип вопросов, которые будут рассматриваться – это вопросы асимптотического поведения этих функций, что может понадобится при оценке сложности теоретико-числовых алгоритмов.

Определение (Арифметические функции)**.** Пусть R — кольцо. Арифметической функцией со значением в R называется отображение $f\colon \mathbb{N} \to R$.

Обычно в качестве R берут комплексные числа. Однако, иногда бывает полезно взять в качестве R кольцо каких-нибудь функций.

Примеры:

1) $1(n) = 1$.

2) $e(n) = \begin{cases} 1, n = 1 \\ 0, \text{ иначе} \end{cases}$.

3) $I_k(n) = n^k$.

4) $\varphi(n)$ — функция Эйлера.

5) И вообще, $f(n) = |V_{g_1,\dots,g_n}(\mathbb{Z}/n)|$, где $g_1, \dots, g_n$ какие-то целочисленные многочлены от одинакового числа переменных.

6) $\sigma(n) = \sum_{d|n} d$

7) Более общо $\sigma_k(n) = \sum_{d|n} d^k$.

8) В частности, $\sigma_0(n) = d(n) = \sum_{d|n} 1$ то есть число делителей.

9) $r(n) = |\{(x, y) \in \mathbb{Z}^2 \,|\, x^2 + y^2 = n\}|$.

Для последовательностей, удовлетворяющих линейным рекуррентным соотношением естественно в качестве производящей функции было взять степенную производящую функцию, так как они ведут себя как геометрическая прогрессия, то с арифметическими функциями дело обстоит иначе. Их величина обычно ограничена полиномом, а то и логарифмом n. Следовательно для их исследований пригодны другие производящие функции.

Определение. Пусть $a\colon \mathbb{N} \to \mathbb{C}$ — арифметическая функция. Производящей функцией Дирихле или рядом Дирихле по s называется следующее выражение

$$L(s) = \sum_{i=1}^{\infty} \frac{a(n)}{n^s}.$$

Определение. В частности знаменитая дзета-функция Римана есть функция Дирихле для $1(n)$ то есть

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Замечание. Если последовательность $a(n)$ есть $O(n^\alpha)$, то ряд Дирихле абсолютно сходится при всех вещественных $s > \alpha + 1$, а на самом деле и при всех комплексных s с $\operatorname{Re} s > \alpha + 1$.

Факт. Пусть $L_1(s)$ – ряд Дирихле для a, а $L_2(s)$ – ряд Дирихле для b. Если ряды L_1 и L_2 сходятся для всех $s > s_0$ и в этой области верно равенство $L_1 = L_2$, то функции a и b равны.

Последние два факта говорят нам, что про ряды Дирихле действительно можно думать, как про честные функции комплексного аргумента. Однако нас больше будет интересовать формальная сторона дела. Тем не менее указанная картинка будет мотивировать нас к некоторым определениям.

Представим себе два ряда Дирихле $L_1(s) = \frac{a_1}{1^s} + \frac{a_2}{2^s} + \dots$ и $L_2 = \frac{b_1}{1^s} + \frac{b_2}{2^s} + \dots$. Перемножим их. Получится выражение вида

$$\sum_{n,m} \frac{a_n b_m}{(nm)^s} = \sum \frac{1}{n^s} \sum_{d|n} a_d b_{\frac{n}{d}}.$$

Это даёт нам основание ввести на всех арифметических функциях структуру умножения не с помощью покомпонентного произведения, а при помощи полученной формулы.

Определение (Свёртка Дирихле)**.** Пусть $a, b\colon \mathbb{N} \to R$ – арифметические функции. Определим их свёртку Дирихле при помощи формулы

$$c_n = \sum_{d|n} a_d b_{\frac{n}{d}} = \sum_{d_1 d_2 = n} a_{d_1} b_{d_2}.$$

Лемма 32. Относительно свёртки Дирихле и поточечного сложения арифметические функции образуют кольцо. Единицей кольца является функция e.

Мы сконцентрируемся сейчас на функциях специального вида.

Определение. Арифметическая функция f называется мультипликативной, если $f(1) = 1$ и для любых двух взаимно простых $(n, m) = 1$

$$f(nm) = f(n)f(m).$$

Возможно вы удивитесь такому определению. Можно было бы ожидать каких-то других слов. Однако именно такая «неполная» мультипликативность встречается очень часто.

Примеры:

Функции примеров 1),2),3),4),5) очевидно или по Китайской теореме об остатках являются мультипликативными. На самом деле функции примеров 6),7),8) и, если чуть-чуть подправить, то 9) так же являются мультипликативными. Попробуем пояснить эти факты.

0.53. Мультипликативность и функция Дирихле. Мультипликативность свёртки.

Прежде всего заметим, что

Лемма 33. Функция f мультипликативна, тогда и только тогда, когда для $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, выполнено $f(n) = \prod f(p_i^{\alpha_i})$.

Лемма 34. Если функция $f\colon \mathbb{N} \to \mathbb{C}$ мультипликативна и $f(n) = O(n^\alpha)$, то её ряд Дирихле раскладывается в произведение при $\operatorname{Re} s > \alpha + 1$

$$L(s) = \prod_{p \text{ простое}} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots\right).$$

Доказательство. Прежде всего заметим, что все ряды $1+\frac{f(p)}{p^s}+\frac{f(p^2)}{p^{2s}}+\dots$ сходятся абсолютно при $\operatorname{Re} s > \alpha+1$. Далее воспользуемся фактом из математического анализа, что произведение двух абсолютно сходящихся рядов сходится к произведению сумм сомножителей. Таким образом, для конечного множества простых S имеет место равенство

$$\prod_{p\in S}\left(1+\frac{f(p)}{p^s}+\frac{f(p^2)}{p^{2s}}+\dots\right)=\sum_{n\in N(S)}\frac{f(n)}{n^s},$$

где $N(S)$ – это множество всех натуральных чисел в чьё разложение входят только простые из S. Возьмём $S_m=\{p\in\mathbb{N}\,|\,p \text{ простое и } p\le m\}$. Переходя к пределу справа и слева, используя абсолютную сходимость ряда $L(s)$, получаем требуемое.

Обратно, если функция $L(s)$ раскладывается в произведение, то

$$L(s)=\lim_{m\to\infty}\prod_{p\in S_m}\left(1+\frac{f(p)}{p^s}+\frac{f(p^2)}{p^{2s}}+\dots\right)=\sum_{\substack{n\in N(S_m)\\ n=p_1^{\alpha_1}\dots p_k^{\alpha_k}}}\frac{f(p_1^{\alpha_1})\dots f(p_k^{\alpha_k})}{n^s}.$$

Предел правого выражения есть функция Дирихле для $g(n)=f(p_1^{\alpha_1})\dots f(p_k^{\alpha_k})$, если $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$, причём, как мы знаем, этот ряд Дирихле абсолютно сходится при $s>\alpha+1+\log c$ где c – константа, что $|f(n)|\le cn^\alpha$, так как

$$|g(n)|\le c^k(p_1^{\alpha_1}\dots p_k^{\alpha_k})^\alpha=O(n^{\alpha+\log c}).$$

Тогда получаем равенство двух рядов Дирихле в области $s>\alpha+1\log c$. Отсюда

$$f(n)=g(n)=f(p_1^{\alpha_1})\dots f(p_k^{\alpha_k}).$$

□

Если мы перемножим две L-функции Дирихле для мультипликативных последовательностей, то получим снова функцию для мультипликативной последовательности. Таким образом должно быть верно

Лемма 35. Свёртка двух мультипликативных функций снова мультипликативна.

Доказательство. Для комплексных последовательностей всё и так доказано. Далее можно воспользоваться принципом про продолжимость полиномиальных тождеств. Но несложно доказать мультипликативность свёртки напрямую:

$$f*g(nm)=\sum_{d|nm}f\left(\frac{nm}{d}\right)g(d)=\sum_{d_1|n,\,d_2|m}f\left(\frac{n}{d_1}\right)f\left(\frac{m}{d_2}\right)g(d_1)g(d_2)=f*g(n)\cdot f*g(m).$$

□

0.54. Обратная функция относительно свёртки...

Обратная функция относительно свёртки. Её мультипликативность. Функция Мёбиуса. Формула обращения.

Теорема 47. Пусть $f\colon\mathbb{N}\to R$, тогда f – обратима тогда и только тогда, когда $f(1)\in R^*$ и обратная функция g задаётся формулой

$$g(n)=\frac{-1}{f(1)}\sum_{d|n,\,d<n}f\left(\frac{n}{d}\right)g(d).$$

Доказательство. Очевидно, что обратимость $f(1)$ необходима. Для того чтобы f и g были обратны необходимо и достаточно, чтобы $g(1)=\frac{1}{f(1)}$ и для каждого $n>1$ было выполнено

$$0=\sum_{d|n}f\left(\frac{n}{d}\right)g(d).$$

Осталось перенести последнее слагаемое в левую часть и поделить на $-f(1)$. □

Лемма 36. Обратная к мультипликативной функции снова мультипликативна.

Доказательство. Проще всего это понять через L-функции. Действительно, каждый сомножитель в разложении в произведение имеет вид $1+\frac{f(p)}{p^s}+\frac{f(p^2)}{p^{2s}}+\dots$ есть ряд от $y=p^s$ начинающийся с единицы. Следовательно, обратный элемент к нему тоже ряд по y. Итого обратная функция тоже раскладывается в аналогичное произведение. Но можно и воспользоваться доказанной формулой про обратную функцию. Рассуждая по индукции, предположим, что для всех пар n_1, m_1 меньших $n, m > 1$ уже показана мультипликативность. Тогда

$$g(nm) = -\sum_{\substack{d|nm\\ d<nm}} f\left(\frac{nm}{d}\right) g(d) = -\sum_{d_1|n}\sum_{d_2|m} f\left(\frac{n}{d_1}\right) g(d_1) f\left(\frac{m}{d_2}\right) g(d_2) + g(n)g(m) = g(n)g(m),$$

так как первое слагаемое есть произведение $e(n)e(m)$. □

Наша задача сейчас описать обратную к функции $1(n)$. Для этого вспомним, что

$$\zeta(s) = \prod\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\dots\right) = \prod\frac{1}{1-p^{-s}}.$$

Тогда $\zeta(s)^{-1}$ имеет вид

$$\zeta(s)^{-1} = \prod\left(1-\frac{1}{p^s}\right).$$

Если раскрыть скобки, то в получившейся сумме не нулевые слагаемые будут только для бесквадратных n, а коэффициент перед ними будет $(-1)^k$, где k – число простых сомножителей.

Определение (Функция Мёбиуса)**.** Определим функцию $\mu(n)$ по следующему правилу

$$\mu(n) = \begin{cases} 0, \text{ если существует простое } p, \text{ что } p^2|n \\ (-1)^k, \text{ если } n = p_1\dots p_k \end{cases}$$

Таким образом функция Мёбиуса обратна к $1(n)$. Это означает, что

Следствие 8. Равенство $f(n) = \sum_{d|n} g(d)$ верно для всех n, тогда и только тогда, когда верно $g(n) = \sum_{d|n}\mu(d)f(\frac{n}{d})$.

Доказательство. По условию $f = g * 1$. Это происходит тогда и только тогда, когда $g = f * 1^{-1} = f * \mu$. □

0.55. Вероятность встретить два взаимно простых числа.

Не имея возможности заниматься комплексным анализом остановимся на простых асимптотических свойствах арифметических функций и каких-нибудь тождествах с ними.

Наша задача — посчитать среднее значение функции Эйлера. Запишем сумму $S_n = \varphi(1)+\dots+\varphi(n)$ и посчитаем её асимптотику. Заметим, что $\varphi(n) = \sum_{d|n}\mu(d)\frac{n}{d}$. Получаем

$$\begin{aligned} S_n &= \sum_{k=1}^{n}\sum_{d|k}\mu(d)\frac{k}{d} = \sum_{dd'\le n}\mu(d)d' = \\ &= \sum_{d\le n}\mu(d)\sum_{d'=1}^{[\frac{n}{d}]}d' = \frac{1}{2}\sum_{d\le n}\mu(d)\left(\left[\frac{n}{d}\right]^2+\left[\frac{n}{d}\right]\right) = \\ &= \frac{1}{2}\sum_{d\le n}\mu(d)\left(\frac{n^2}{d^2}+O\left(\frac{n}{d}\right)\right) = \frac{1}{2}\sum_{d\le n}\mu(d)\frac{n^2}{d^2}+O\left(n\sum\frac{1}{d}\right) = \\ &= \frac{n^2}{2}\sum_{d\le n}\frac{\mu(d)}{d^2}+O\left(n\log n\right) = \frac{n^2}{2}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O(n)+O(n\log n) = \frac{3n^2}{\pi^2}+O(n\log n) \end{aligned}$$

Заметим, что сумма S_n это так же количество взаимно простых чисел p, q, что $1 \le p < q \le n$. Количество вообще пар чисел, что $1 \le p < q \le n$ есть $\frac{1}{2}n(n+1)$. Отсюда получаем, что при больших n вероятность выбрать два взаимно простых числа есть $\frac{6}{\pi^2}$.