

01) Определение алгебры кватернионов. Векторное произведение. Сопряжённый кватернион. Норм кватерниона. Мультипликативность нормы. Сумма четырёх квадратов.  
 $uv = -\langle u, v \rangle + [u, v]; \|x\| = \sqrt{\det x}; n_1 n_2 = \|a\|^2 \|b\|^2 = \|ab\|^2.$

02) Свойства сопряжения и векторного произведения.  
 Определение  $\bar{x}$ . Важные выражения:  $[v, v], [v, u] + [u, v]$ , для чисто мнимых:  $u^2, u[u, v], \|[u, v]\|.$

03) Кватернионы и вращения  $R^3$   
 $H_1; t = a + bu$ , условия на  $u, a^2 + b^2; xy = [x, y]; x^{-1}, \bar{x}; x^2, \|x\|; \|a + bx\|$ . Определение угла, поворота.

04) Максимум квадратичной формы на сфере. Теорема Куранта-Фишера.  
 Норм и матанализ. Собственные числа. Подпространства размерности  $k$ .

05) Оценка на собственные числа ограничения. Оценка на след.  
 1. С.ч. операторов  $A$  и  $B$ . По КФ, мин/макс для  $\mu_i$  берется по подпр. внутри соотв. подпр. для  $\lambda$  (NB:  $\lambda_{i+n-m}$ ). 2. Это след: взять матрицу  $A$  в ортонорм. базисе  $u_i$ .  $v_i = (0, \dots, 1, \dots, 0)^T$ .  $A_{i,i} = v_i^T A v_i = q(u_i)$ . Оценка: почленные нер-ва из 1.

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

07) Сингулярные значения и SVD-разложение.  
 $X^* = X^T, \langle X^* e_i, e_j \rangle = \langle e_i, X e_j \rangle, \sigma_i = \sqrt{d_i} > 0$  с.ч.  $A^* A$ . SVD  $A: U \rightarrow V \exists$  о/н  $u_i, v_j$ : матр  $A = \Sigma(\sigma_{1..r}$  на диаг)  $(X = L \Sigma R)$ .  $e_i$  - о/н с.в.  $\langle A e_i, A e_j \rangle = \langle A^* A e_i, e_j \rangle = \langle d_i e_i, e_j \rangle, f_i = \frac{A e_i}{\sqrt{d_i}}$  доп до базиса.  $R = C^{-1} = C^T, C$  столбцы  $e_i$ .

08) Приближение матрицей указанного ранга и SVD-разложение. Возможность применения к сжатию изображений.  
 рг из Б6  $\Leftrightarrow$  близ по  $\|X\|_F = \sqrt{\text{Tr } X^T X}$ .  $X = L \Sigma R$ . рг на  $\langle v_1^T \dots v_k^T \rangle$ .  $v_i$  базис  $X^T X$  и строки  $R$ . рг  $a$  на  $V^{(k)} = \sum a v_i v_i^T$ .  $X^{(k)} = L \Sigma(\sum R v_i v_i^T) = L \Sigma R^{(k)} = L \Sigma^{(k)} R$ . Сж  $L^{(k)} \Sigma^{(k)} R^{(k)}$ .  $2kn + k \rightarrow 2kn$  при  $k < \frac{n}{2}$ . Минор  $k^2 + 2k(n - k) + 2k$ .

09) Положительные матрицы. Теорема Перрона.  
 Док-во Перрона: полож-ть  $(A|x| \geq |x| \Rightarrow Ay > \varepsilon z, z = A|x| \Rightarrow A|x| < \frac{A^n}{(1+\varepsilon)^n} A|x| \rightarrow 0$  противореч.), ед-ть (сонапр. коорд.  $v \Leftarrow \sum_j A_{kj} |v_j| = |\sum_j A_{kj} v_j|$ ) и некра-ть (Жорд. клетки; либо  $\exists c, i: |x_1 - c x_2|_i = 0$ , либо  $A x_2 = x_2 + x_1$ )

10) Единственность положительного собственного вектора. Применение к случайному блужданию.  
 1. См.  $\lambda x^T y$ . 2. Знаем предел  $\lim_{k \rightarrow \infty} A^k v$ , если у  $A$  макс по модулю с. ч.  $\lambda = 1$  кратности 1.  $P(G): P_\alpha(G) = (1 - \alpha)P(G) + \alpha \frac{1}{n} J$ ,  $\alpha \in (0, 1)$ ,  $\forall i, j$   $J_{ij} = 1 - \alpha$  это норм, Перрон гарантирует (см  $(1, \dots, 1)$ ).

12) Сильно регулярные графы. Граф Петерсона и его спектр. Двудольность и спектр.  
 $A^2 + (\mu - \lambda)A + (\mu - k)E = \mu J$ ,  $A_{|U}^2 + (\mu - \lambda)A_{|U} + (\mu - k)E = 0$  для  $U = \langle (1, \dots, 1) \rangle^\perp$   
 След степени == количество циклов == сумма собственных чисел с учетом кратности.  $\lambda$  для  $(v, w)$ ,  $-\lambda$  для  $(v, -w)$

13) Две оценки на размер максимального независимого множества.  
 Натянуть подпространство на множество, следствие из КФ, нулевая квадратичная форма  
 Характеристический вектор множества, разложить по ортонорм. базису регулярного(!) графа с  $u_1 = (1, \dots, 1) \frac{1}{\sqrt{n}}$

14)  $K_{10}$  не покрывается тремя Петерсонами.  
 $\sum_{i=1}^3 A_i = B$ . Все рег  $\Rightarrow$  общий с.в.  $(1, \dots, 1)$  для  $P$  с.ч. 3, для полного с.ч. 9. Сузим. Для  $A_1$  и  $A_2$  подпр. породж. с.в. с с.ч. 1  $\cap$ . Распишем для  $u$  из  $\cap$ .  $Bu = -u$  (натянута на с.в. с с.ч.  $-1$ ).  $\Rightarrow$  с.в. для  $A_3$  с с.ч.  $-3$ . Такого с.ч. нет.

15) Тензорное произведение. Существование.  
 $\cong K \langle V_1 \times \dots \times V_n \rangle / K \{ (\dots \lambda v + u \dots) - \lambda(\dots v \dots) - (\dots u \dots) \} = T$ .  $\forall h: K \langle \times V_i \rangle \rightarrow U \exists \hat{h}: \otimes V_i \rightarrow U, \hat{h} \circ i = h, \hat{h}((v_1, \dots)) = h(v_1, \dots)$   
 однозначно и пропускается через  $T$ , т. к. все соотн в ядре (проверить).  $\hat{h}(v_1 \otimes \dots) = \hat{h}((v_1, \dots))$ .  $h$  - полилин,  $\hat{h}$  - лин.

16) Единственность тензорного произведения. Размерность тензорного произведения.  
 Единств: рассм полилин отобр  $i_1$  и  $i_2$  для  $\otimes_1$  и  $\otimes_2$  из опр.  $\exists \hat{i}_1, \hat{i}_2: \hat{i}_1 \circ i_2 = i_1, \hat{i}_2 \circ i_1 = i_2$ . Д-ть, что  $\hat{i}_1 \hat{i}_2 = \text{Id}$ . Разм:  $e_{1j_1} \otimes \dots \otimes e_{1j_n}$  породж (раскр по полилин).  $\text{Hom}(V_1, \dots, V_n, K) \cong \text{Hom}(V_1 \otimes \dots \otimes V_n, K) \cong V_1 \otimes \dots \otimes V_n$ .

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

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

18) Канонические изоморфизмы для тензорного произведения.

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

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

$(p,0)$  – полилин. форма,  $(1,1)$  – лин. оп-р,  $(2,1)$  – структ. алгебры. Переход:  $x_{new} = Cx_{old}$ .  $e_i = \sum_{j=1}^n C_{ji} \hat{e}_j$ , хотим  $D : e^i = \sum D_{ji} \hat{e}^j$ .  $e^k(e_i) = \delta_{ki} \Rightarrow \delta_{ki} = \sum_j C_{ji} \sum_l D_{lk} \hat{e}^l(\hat{e}_j) = \sum_{j,l} C_{ji} D_{lk} \cdot \delta_{lj} = \sum_j C_{ji} D_{jk}$   $E_n = C^T D \Rightarrow D = (C^{-1})^T$

20) Замена переменной – общий случай.

$T = \sum_{\substack{i'_1, \dots, i'_q \in \overline{1, n} \\ j'_1, \dots, j'_p \in \overline{1, n}}} T_{j'_1, \dots, j'_p}^{i'_1, \dots, i'_q} e_{j'_1, \dots, j'_p}^{i'_1, \dots, i'_q}$ .  $e_i = \sum_{j=1}^n C_{ji} \hat{e}_j$  и  $e^i = \sum D_{ji} \hat{e}^j$ . Раскрыть скобки, поменять суммирование. Должно

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

21) Тензорная алгебра. Свёртка и след.

Для  $(1,1)$   $T = \sum_{i,j} T_j^i e^j \otimes e_i$ . Тогда  $\text{Conv}(T) = \sum_{i,j} T_j^i e^j(e_i) = \sum_i T_i^i$ .  $V^* \otimes V \cong \text{Hom}(V, V) \Rightarrow$  это след.

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

Лемма: Пусть нет, возьмём  $\min a_i, b_j \nmid p$ , тогда  $c_{i+j} \nmid p$ . Содержание: поделим на  $\text{cont } g, h$ , убедимся что  $\text{cont } f = 1$ . Лемма про  $Q(R)[x]$ :  $d_1, d_2$  – НОК знаменателей,  $c = \frac{d_1}{d_2}$ .

28) Факториальность кольца многочленов над факториальным кольцом.

$R[x]$  факториально и простые в нём:  $f = p \in R$ ,  $f : \text{cont}(f) = 1$  – непр. в  $Q(R)[x]$ . 1) Б27 2) в них раскладывается, посмотрим в  $Q(R)$ ,  $g = \frac{a_1}{a_2} f q \Rightarrow \frac{a_1}{a_2} q \in R[x]$  (т.к.  $\text{cont}(q) : a_2$ ) 3)  $f = a \prod g_i$

29) Редукционный признак неприводимости. Примеры. Признак Эйзенштейна.

1.  $a_n \nmid p$ ,  $f$  – неприводим в  $R/p[x] \Rightarrow$  неприводим над  $Q(R)$ .  $\text{cont} = 1$  и непр-ть над  $Q(R) \Rightarrow$  непр-ть над  $R$  (см. степени  $g$  и  $h$ ). 2.  $a_n \nmid p$ , все  $a_i : p \mid i < n$ , но  $a_0 \nmid p^2$ , то многочлен  $f(x)$  неприводим. Пусть  $b_0 \nmid p$ , см.  $\min c_s \nmid p$  и  $a_s$ .

30) Алгоритм Кронекера. Сведение для многочленов от нескольких переменных.

1) Перебираем наборы делителей  $f(i)$ ,  $0 \leq i \leq \frac{\deg f}{2}$ , интерполируем, проверяем. 2) Различными разложениям  $f(x_1, \dots, x_n)$  соответствуют различные разложения  $f(x, \dots, x^{d^{n-1}})$  для  $d$  больших  $\max_{i=1}^n \{\deg_{x_i} f\}$ . Рассмотреть образ  $x^\alpha$ .

31) Лемма Гензеля. Разложение на множители при помощи леммы Гензеля.

Доказательство леммы: Индукция по  $k$ . Строим для  $k+1$ . Помним, что  $\forall f : p^k f \equiv p^k \bar{f} \pmod{p^{k+1}}$ .

$\bar{h} \equiv \bar{h} + p^k a(x) \Rightarrow \bar{h} \bar{g} \equiv \bar{g} \bar{h} + p^k(a(x)g + b(x)h)$ . С другой стороны  $f - \hat{g}h = p^k c(x) \Rightarrow a, b$  берем из лп НОДа  $g$  и  $h$

32) Степенные суммы. Тождество Ньютона.

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

33) Целые алгебраические элементы. Замкнутость относительно операций.

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

37) Описание наименьшего подрасширения, содержащего данный элемент.

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

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  $4x^3 - 3x = \frac{1}{2}$ .

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

1. Содержит  $Z/p$  2.  $p^n$  эл-тов (см. как п/г по +) 3. См. на мультипл. группу. Теорема Ферма для групп. 4. Биномиальный коэф. делится на  $p$  почти всегда. 5. Аккуратно всё проверить.

40) Основная теорема про конечные поля.

Поле разложения  $x^{p^n} - x \rightarrow$  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.

41) Подполя данного конечного поля. Описание автоморфизмов  $F_p^n$ .

1.  $\mathbb{F}_{p^n} \in \mathbb{F}_{p^m}$ : а) Башня б) см.  $\{x \in \mathbb{F}_{p^m} | x^{p^n} - x = 0\}$ , это подполе,  $p^n$  эл-тов, т.к.  $x^{p^m} - x : x^{p^n} - x$  и первый раскладывается на лин. множители. 2.  $\mathbb{F}_q = \mathbb{F}_p[\alpha]$ , где степень мин.  $f$  для  $\alpha$  равна  $n$ , а авт-м задаётся образом корня.

42) Распирения поля  $F_q$ . Неприводимые многочлены как делители  $x^{q^d} - x$ .

1.  $q^{[L:\mathbb{F}_q]}$ , существ. по Б41. Изоморф-м  $L_1$  и  $L_2$ : знаем для  $\mathbb{F}_p$  (Б40),  $\varphi(\mathbb{F}_q) = \mathbb{F}_q \Rightarrow$  это степень Frob, см. обратный к нему над  $L_2$ . 2. а)  $\mathbb{F}_q[\alpha] \in \mathbb{F}_{q^m}$  (т.к. есть корень), Башня. б) см.  $\mathbb{F}_{q^{\deg f}} \cong \mathbb{F}_q[x]/f \Rightarrow$  общий  $\alpha$  (NB:  $f$  – неприводим).

43) Лемма про производную. Лемма про эффективное извлечение корня степени  $p$ .

1.  $f = \prod g_i^{n_i}$ , смотрим  $f = g_i^{n_i} g$ , берём произв., см. на степень вхождения в  $f$  и  $f'$ . 2.  $h' = 0 \Leftrightarrow h = g(x^p)$ , коэфф.  $g$ :  $a_i$ , см.  $b_i^p = a_i$  (можно, т.к. Frob), см.  $f$  с коэфф.  $b_i$  и распиши  $f^p = g(x^p) = h$ . Для извлечения см. обратный Frob.

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

См. Б42 про критерий для степени. Инд-ция: пусть на шаге у  $f$  нет мн-лей степени  $< l$ .  $g(x) = x^{q^l} - x$ , НОД( $g, f$ ) состоит из мн-лей  $f$  степени  $= l$ , т.к. делит, а меньше нет. НОД( $g, f$ ) = НОД( $r, f$ ). Значит нужно  $x^{q^l} \bmod f$  (см. в  $\mathbb{F}_q[x]/f$ ).

45) Алгоритм Берлекэмп.

$R = \mathbb{F}_q[x]/f \cong \prod \mathbb{F}_q[x]/h_i$ . Хотим дел-ли 0. Смотрим на  $\{y \in \mathbb{F}_q[x]/f | y^q - y = 0\}$  (покомпонентно удовл-т). Это линейное  $\Rightarrow$  есть матрица, её решаем, получаем  $l$ -ку коэфф. Перебираем константы, обнуляем координату, см. на НОД с  $f$ .

46) Вероятностный алгоритм Кантора-Цассенхауза.

1. Про кв-ты:  $x^{\frac{q^d-1}{2}} = \pm 1$ . 2. Как в Б45, такое же  $R$ , отсюда случ-й  $h \rightarrow h^{\frac{q^d-1}{2}} - 1$ . Попадём в  $\{0, -1, -2\}$ . Худший случай:  $\mathbb{F}_3 \times \mathbb{F}_3$ . Считаем вероятность получить среди первых двух комп-т квадрат и не квадрат ( $p \geq \frac{4}{9}$ ).

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

Хэмминг, код, кодовое расстояние, обнаруживает, исправляет,  $n$ - $k$ - $q$ -код, линейному соответствует матрица, систематический, проверочная матрица (образ – её ядро), мин. число ненулевых координат  $x$  = кол-во нез. столбцов.

49) Циклические коды. Эквивалентное описание. Коды БЧХ. Пример.

$q = p^s$ ,  $m, n$  такие, что  $q^m - 1 : n$ ,  $2 \leq d \leq n$ ,  $l_0 \leq n$ .  $\alpha$  – образующая  $\mathbb{F}_{q^m}^*$ ,  $\beta = \alpha^{(q^m-1)/n}$   
Пример:  $q = 2, m = 4, l_0 = 1, n = 15, d = 5, f = x^4 + x^3 + 1$ .

50) Основная теорема про коды БЧХ.

1. Делится  $\Leftrightarrow$  обнуляется на корнях, определитель  $p(x) \rightarrow p(\beta^i)$ . 2.  $d_{\min} \geq d$ . Пусть плохо  $\mathbb{F}_q$ , тогда плохо в  $\mathbb{F}_{q^m}$ , обнуляет  $H \Rightarrow$  у неё есть  $d - 1$  зависимый столбец, выделим их, сведём к Вандермонду, не вырождено.

51) Алгоритм декодирования Питерсона-Горенштейна-Цирлера.

$e(x) = \sum e_{ij} x^{ij}$ . Расписать через  $Y_j X^{l_0+k-1}$ . Хотим  $Y_j$ , значит нужны  $X$ . См.  $\Lambda(x) = \prod (1 - x\Lambda_i)$ . Хотим  $\Lambda_i$ , тогда найдём корни и обратим. См.  $0 = \Lambda(X_j^{-1})$ , домножаем на  $Y_j X_j^{\nu+t}$ , суммируем  $(l_0..l_0 + t - 1)$ , меняем на  $S_{t+1}..S_{2t}$ .

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

1.  $f(1)$  – обратимо, выкидываем  $n$ , см.  $0 = \sum_{d|n} f(\frac{n}{d})g(d)$ . 2. Инд-ция по  $(n, m)$ :  $g(nm) = - \sum_{d|nm, d < nm} \frac{nm}{d} g(d) = e(n)e(m) + g(n)g(m)$ . 3. Пишем дзета-ф-цию, суммируем как БУГП, см. обратную. 4.  $f = g * 1 \Leftrightarrow g = f * 1^{-1} = f\mu$ .

55) Вероятность встретить два взаимно простых числа.

Считаем  $\sum \varphi(i), \varphi(n) = \sum \mu(d) \frac{n}{d}$ . Дальше аккуратно считаем, разбиваем на две суммы (по  $\mu(d)$  и  $d'$ ), в конце  $\frac{n^2}{2} \sum \frac{\mu(d)}{d^2} = \frac{3n^2}{\pi}$