ЧЕТЫРНАДЦАТАЯ СТУДЕНЧЕСКАЯ ОЛИМПИАДА ПО АЛГЕБРЕ НА МЕХМАТЕ МГУ. РЕШЕНИЕ ЗАДАЧ

1. Назовём элемент квадратной матрицы *важным*, если определитель этой матрицы можно изменить, изменив только этот элемент.

а) Существует ли вещественная матрица сто на сто, содержащая ровно два важных элемента?

б) Сколько существует матриц 6×6 над $\mathbb{Z}_2$ $(= \mathbb{F}_2)$, содержащих ровно пять важных элементов?

Предложили А. Л. Канунников и А. А. Клячко.

Решение. а) Да (для любого размера, начиная с два на два): $\begin{pmatrix} \boxed{0} & \boxed{0} & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$.

В пункте б) ответ такой: $72 \cdot 31 \cdot 30 \cdot 28 \cdot 24 \cdot 16$. Чтобы в этом убедиться, докажем сперва следующее утверждение.

Утверждение 1. *Пусть матрица $A \in \mathrm{M}_n(K)$, где K — поле и $n \geqslant 3$, содержит ровно p важных элементов, где p — простое число и $p < n$. Тогда $\operatorname{rank} A = n - 1$, в матрице A есть нулевая строка или нулевой столбец, и все важные элементы лежат в этой строке (в этом столбце).*

Доказательство. Так как $p < n$, то в A есть строка из неважных элементов. Соответствующая строка в присоединённой матрице $\widehat{A}$ (состоящей из алгебраических дополнений к элементам матрицы A) нулевая, поэтому $\operatorname{rank} A < n$. Значит, $\operatorname{rank} A = n - 1$ (иначе важных элементов нет), откуда $\operatorname{rank} \widehat{A} = 1$. Число ненулевых элементов присоединённой матрицы по условию равно простому числу, поэтому все они лежат в одной строке или в одном столбце (иначе мы имели бы две непропорциональные строки или два непропорциональных столбца и $\operatorname{rank} \widehat{A}$ был бы больше единицы). Без ограничения общности можно считать, что они лежат в первой строке (этого можно добиться транспонированием и/или перестановкой строк).

Вычеркнув из матрицы A любую i-ю строку с $i > 1$, получим матрицу ранга $< n - 1$, поскольку все её миноры порядка $n - 1$ равны нулю (иначе в i-й строке был бы важный элемент). Значит, есть только одна база строк матрицы A — все строки без первой. Отсюда следует, что первая строка нулевая, и утверждение доказано.

Пусть теперь $K = \mathbb{Z}_2$ и $n = p + 1$ в условиях утверждения 1. Сосчитаем число таких матриц. Положение важных элементов можно выбрать $2(p+1)^2$ способами: номер строки или номер столбца $(2(p+1)$ вариантов) и номер единственного неважного элемента в выбранной строке/выбранном столбце $(p + 1$ вариантов). Пусть $a_{11}, \ldots, a_{1p}$ — важные элементы и $\overline{A}$ — матрица, полученная из A вычёркиванием первой строки, $a_1, \ldots, a_{p+1}$ — столбцы матрицы $\overline{A}$. Тогда $\operatorname{rank}\{a_1, \ldots, a_{p+1}\} \setminus \{a_i\} = p$ при всех $i = 1, \ldots, p$ и $\operatorname{rank}\{a_1, \ldots, a_p\} = p - 1$. Это равносильно тому, что

1) столбцы $a_2, \ldots, a_{p+1}$ линейно независимы;
2) столбец a_1 выражается через $a_2, \ldots, a_p$, но не выражается через меньшее число столбцов, т. е., с учётом условия 1) и того, что $K = \mathbb{Z}_2$, $a_1 = a_2 + \ldots + a_p$.

Таким образом, число подходящих матриц $\overline{A}$ равно $|\mathbf{GL}_p(\mathbb{Z}_2)|$. Окончательный ответ:

$$2(p+1)^2 |\mathbf{GL}_p(\mathbb{Z}_2)| = 2(p+1)^2 (2^p - 1)(2^p - 2) \ldots (2^p - 2^{p-1}).$$

Осталось подставить $p = 5$.

2. Назовём *корнями* из перестановки все перестановки, которые в квадрате равны данной.

а) Для каких натуральных чисел k есть перестановка (в какой-нибудь конечной симметрической группе S_n) такая, что из неё есть ровно k различных корней?

б) Верно ли, что для любой перестановки из S_n количество корней из неё не превосходит количества корней из тождественной перестановки?

Предложил С. А. Гайфуллин

Решение. В пункте а) ответом служит множество $\{1\} \cup 2\mathbb{N}$. Единица очевидно является числом корней из тождественной перестановки в S_1. А чётное число $2k$ является числом корней из произведения двух независимых циклов $(1\ 2\ \ldots\ k)(k+1\ k+2\ \ldots\ 2k)$ длины k в S_{2k}. Действительно, все корни из этого произведения являются следующими циклами длины $2k$:

$(1\ k+1\ 2\ k+2\ \ldots\ k\ 2k)$, $(1\ k+2\ 2\ k+3\ \ldots\ k\ k+1)$, $(1\ k+3\ 2\ k+4\ \ldots\ k\ k+2)$, $\ldots$, $(1\ 2k\ 2\ k+1\ \ldots\ k\ 2k-1)$.

Теперь покажем, что

нечётное число большее единицы не может быть числом корней ни из какого элемента g никакой группы G.

Заметим, что все эти корни должны коммутировать с g, то есть лежать в централизаторе $C(g)$ элемента g. Если порядок группы $C(g)$ нечётен, то из любого элемента этой группы корень извлекается единственным образом. Если же $|C(g)|$ чётный, то по лемме Коши (по теореме Силова, если угодно) в $C(g)$ найдётся элемент d порядка два.*) Это позволяет устроить следующее отображение f из множества $\sqrt{g} \stackrel{\text{опр}}{=} \{x \in G \mid x^2 = g\}$ корней из g в себя:

$$f(x) = \begin{cases} dxd^{-1}, & \text{если } dx \neq xd; \\ dx, & \text{если } dx = xd. \end{cases}$$

Ясно, что это инволюция, то есть $f(f(x)) = x$ всегда, и неподвижных точек она не имеет, то есть $f(x)$ не равно x никогда. Отсюда следует, что число элементов в множестве $\sqrt{g}$ чётно.

В пункте б) ответ **Да**. Это немедленно вытекает из следующего факта

Факт. *Для любой перестановки $\sigma \in S_n$ отображение $f\colon (i_1\ i_2\ \ldots)(j_1\ j_2\ \ldots)\ldots \mapsto (i_1\ i_2)(j_1\ j_2)\ldots$, где $i_1 = \min\{i_s\}$, $j_1 = \min\{j_s\}, \ldots$, является инъективным отображением из $\sqrt{\sigma}$ в $\sqrt{e}$.*

Доказательство. Если $\alpha^2 = \sigma$ и $f(\alpha) = (i_1\ i_2)(j_1\ j_2)\ldots$, то перестановка α обязана иметь вид

$$\Big(i_1\ i_2\ \sigma(i_1)\ \sigma(i_2)\ \sigma^2(i_1)\ \sigma^2(i_2)\ \sigma^3(i_1)\ \sigma^3(i_2)\ \ldots\Big)\Big(j_1\ j_2\ \sigma(j_1)\ \sigma(j_2)\ \sigma^2(j_1)\ \sigma^2(j_2)\ \sigma^3(j_1)\ \sigma^3(j_2)\ \ldots\Big)\ldots$$

Другое решение пункта а) (ведущее к явному подсчёту числа корней из перестановки). Для $\sigma \in S_n$ обозначим $\sqrt{\sigma} = \{\tau \in S_n \mid \tau^2 = \sigma\}$. Пусть $f(m, i)$ — число корней из произведения m независимых циклов длины i.

1. Если τ — цикл нечётной длины $2j-1$, то τ^2 — цикл той же длины, причём τ однозначно восстанавливается по τ^2: $\tau = (\tau^2)^j$. Поскольку циклы чётной длины не являются квадратами, то

$$f(1, i) = \begin{cases} 0 & \text{при чётном } i \\ 1 & \text{при нечётном } i. \end{cases} \tag{1}$$

2. Если τ — цикл чётной длины $2j$, то τ^2 — произведение двух циклов длины j, причём квадраты ровно j циклов дают $\tau^2 = (p_1 \ldots p_j)(q_1 \ldots q_j)$: $(p_1 q_{t+1} p_2 q_{t+2} \ldots p_j q_{t+j})$, $t \in \mathbb{Z}_p$. Кроме того, при нечётном j квадрат ещё одной перестановки равен τ^2: $\sqrt{(p_1 \ldots p_j)}\sqrt{(p_1 \ldots p_j)}$. Таким образом,

$$f(2, i) = f(1, i) + i. \tag{2}$$

3. Пусть $\sigma = c_1 \ldots c_m$, где $c_1, \ldots, c_m$ — независимые циклы длины i, и $\tau^2 = \sigma$. Тогда либо c_1 — квадрат некоторого цикла в τ (что возможно лишь при нечётном i) — тогда $\tau \in \sqrt{c_1}\sqrt{c_2 \ldots c_m}$, либо при некотором $k = 2, \ldots m$ произведение $c_1 c_k$ — квадрат некоторого цикла C в τ — тогда $\tau C^{-1} \in \sqrt{c_2 \ldots \widehat{c_k} \ldots c_m}$, причём C можно выбрать i способами по пункту 2. Таким образом,

$$f(m, i) = f(1, i) f(m-1, i) + (m-1) i \underbrace{f(m-2, i)}_{1 \text{ при } m=2}. \tag{3}$$

4. Для любой перестановки σ обозначим через σ_i произведение всех m_i независимых циклов длины i в разложении σ и через X_i — множество элементов этих циклов. Подчеркнём, что под σ_i мы понимаем перестановку с областью определения X_i, $\{1, \ldots, n\} = X_1 \sqcup X_2 \sqcup \ldots$, $|X_i| = m_i i$. Поскольку при извлечении корня из σ циклы из разных σ_i не сливаются, то

$$\sqrt{\sigma} = \prod_i \sqrt{\sigma_i} \Longrightarrow |\sqrt{\sigma}| = \prod_i |\sqrt{\sigma_i}| = \prod_i f(m_i, i).$$

Из (1), (2) и (3) получаем:

$$f(2, i) = f(1, i) + i \vdots 2 \Longrightarrow f(3, i) = f(1, i) f(2, i) + 2 i f(1, i) \vdots 2 \Longrightarrow f(m, i) \vdots 2 \text{ при } m \geqslant 4.$$

С другой стороны, $f(1, 1) = 1$ и $f(2, 2j) = 2j$. Значит, когда σ пробегает все чётные перестановки, $|\sqrt{\sigma}|$ пробегает $\{1\} \cup 2\mathbb{N}$.

---

*) Тем, кто не знаком ни с леммой Коши, ни с теоремой Силова, предлагается самостоятельно доказать следующий элементарный факт: *если из перестановки σ корень извлекается неоднозначно, то найдётся перестановка d порядка два, коммутирующая с перестановкой σ.* Чуть ниже можно найти другое решение этой задачи.

3. Может ли множеством всех значений многочлена от двух переменных с действительными коэффициентами быть множество всех положительных чисел? *Предложил А. Л. Канунников.* (Это очень старая задача. Некоторое развитие этой темы можно найти здесь: https://mathoverflow.net/q/38019/24165 .)

Решение. Да: $(1-xy)^2+x^2$.

4. Студент Двоечкин убеждён, что вещественные векторы $v_1,\dots,v_k$ называются линейно независимыми, если из равенства $\sum\lambda_i v_i=0$ (где $\lambda_i\in\mathbb{R}$) вытекает, что $\sum\lambda_i=0$. Может ли конечное множество векторов содержать меньше базисов, чем *Д-базисов* (то есть максимальных по включению линейно независимых в смысле Двоечкина подмножеств)? *Предложил А. А. Клячко.*

Решение. Нет, не может, поскольку

каждый Д-базис содержит по меньшей мере один базис; а каждый базис содержится ровно в одном Д-базисе.

Первое из этих утверждений вытекает из того, что Д-независимость сохраняется при добавлении к множеству векторов $\{v_1,\dots,v_k\}$ вектора, не выражающегося через $v_1,\dots,v_k$.

Для доказательства второго утверждения возьмём какой-то базис B множества векторов X и покажем, что множество векторов с единичной суммой координат $D=\left\{x\in X\;\middle|\;x=\sum\limits_{b\in B}\lambda_{b,x}b,\ \sum\limits_{b\in B}\lambda_{b,x}=1\right\}$ является единственным Д-базисом множества X, содержащим B. Действительно, множество D является Д-независимым: если $\sum\limits_{d\in D}\mu_d d=0$, то $\sum\limits_{d\in D}\mu_d\lambda_{b,d}=0$, для каждого $b\in B$ и, следовательно,

$$0=\sum_{b\in B}\sum_{d\in D}\mu_d\lambda_{b,d}=\sum_{d\in D}\mu_d\sum_{b\in B}\lambda_{b,d}=\sum_{d\in D}\mu_d,\quad\text{что и требовалось.}$$

С другой стороны, любое Д-независимое множество векторов из X, содержащее B, обязано содержаться в D, так как, если $x=\sum\limits_{b\in B}\lambda_{b,x}b$ и $\sum\limits_{b\in B}\lambda_{b,x}\neq 1$, то равенство $x-\sum\limits_{b\in B}\lambda_{b,x}b=0$ показывает, что любое множество векторов, содержащее $B\cup\{x\}$, Д-зависимо.

5. Покажите, что число неизоморфных конечных групп, содержащих менее миллиона классов сопряжённости, конечно. *Предложил А. А. Клячко.* (Этот факт «широко известен в узких кругах»: https://groupprops.subwiki.org/wiki/There_are_finitely_many_finite_groups_with_bounded_number_of_conjugacy_classes .)

Решение. Группа G разбивается на классы сопряжённости, а мощность каждого из этих классов есть индекс централизатора элемента из этого класса: $|G|=\sum\limits_{i=1}^{k}|G|/|C(g_i)|$. Деля на $|G|$, получаем разложение единицы в сумму египетских дробей: $1=\sum\limits_{i=1}^{k}1/n_i$, где $n_i\in\mathbb{N}$. Осталось показать, что при фиксированном k имеется лишь конечное число таких разложений (поскольку $\max\limits_j(|G|/|C(g_i)|)=|C(e)|=|G|$, а групп данного порядка конечное число). Эта школьная задачка легко решается:

при любом фиксированном $k\in\mathbb{N}$ каждое рациональное число допускает лишь конечное число разложений в сумму k египетских дробей.

Индукция по k. Если мы ищем всевозможные разложения $q=1/n_1+\ldots+1/n_k$, то ясно, что $\min\{n_i\}\leqslant k/q$. Поэтому разность $q-1/\min\{n_i\}$ принимает лишь конечное число значений, каждое из которых может быть разложено в сумму $(k-1)$-й египетской дроби лишь конечным числом способов по предположению индукции.

6. Покажите, что в каждой неединичной конечной группе найдётся элемент, не сопряжённый своему квадрату. *Предложил А. А. Клячко.*

Решение. Пусть p — минимальный простой делитель порядка группы G. По теореме Силова (по лемме Коши, точнее говоря) найдётся элемент $g\in G$ порядка p. Если бы g был сопряжён с g^2, то сопрягающий элемент h действовал бы нетривиальным автоморфизмом на $\langle g\rangle_p$ и, следовательно, по теореме о гомоморфизмах, применённой к отображению $\langle h\rangle\to\operatorname{Aut}\langle g\rangle$, $h^k\mapsto\left(x\mapsto h^kxh^{-k}\right)$, нетривиальная факторгруппа группы $\langle h\rangle$ вкладывалась бы в $\operatorname{Aut}\mathbb{Z}_p$, и $|\langle h\rangle|$ был бы не взаимно прост с числом $|\operatorname{Aut}\mathbb{Z}_p|=|\mathbb{Z}_p^*|=p-1<p$, что невозможно по теореме Лагранжа (из-за минимальности p).

7. Покажите, что целочисленная матрица A подобна (в $\mathbf{GL}_n(\mathbb{R})$) ортогональной матрице тогда и только тогда, когда $A^m = E$ для некоторого натурального m. Верно ли аналогичное утверждение для матриц с рациональными элементами? (E — это единичная матрица.) *Предложил А. А. Клячко.*

Решение. Матрица из $\mathbf{GL}_n(\mathbb{R})$

- подобна ортогональной в точности тогда, когда она диагонализируема над $\mathbb{C}$ и все её собственные значения по модулю равны единице;
- имеет конечный порядок в точности тогда, когда она диагонализируема над $\mathbb{C}$ и все её собственные значения являются корнями из единицы.

Таким образом, матрицы конечного порядка подобны ортогональными. Обратное верно не для любых матриц из $\mathbf{GL}_n(\mathbb{Q})$. Покажем, например, что ортогональная матрица $A = \frac{1}{5}\begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix}$ имеет бесконечный порядок. В самом деле, если $A^m = E$, где $m \in \mathbb{N}$, то аннулирующий многочлен $t^m - 1$ матрицы A делится на её минимальный многочлен $t^2 - \frac{6}{5}t + 1$, что невозможно в силу следующего утверждения.

Факт. *Любой делитель многочлена с целыми коэффициентами и старшим коэффициентом один, имеющий рациональные коэффициенты и старший коэффициент один, имеет целые коэффициенты.*

(Это легко следует из теоремы Гаусса о примитивности произведения примитивных многочленах.)

Покажем, что целочисленная матрицы A, подобная ортогональной, имеет конечный порядок. Для всех $k \in \mathbb{N}$ имеем:

$$\chi_{A^k}(t) = |tE - A^k| = (t - \lambda_1^k)\dots(t - \lambda_n^k) \in \mathbb{Z}[t],\ |\lambda_1| = \dots = |\lambda_n| = 1.$$

Но приведённых многочленов над $\mathbb{Z}$ степени n, все корни которых по модулю равны 1, конечное число, так как их коэффициенты ограничены по модулю 2^n, что следует из формул Виета и оценки

$$|x_1|, \dots, |x_n| = 1 \Longrightarrow \left| \sum_{i_1 < \dots < i_k} x_{i_1} \dots x_{i_k} \right| \leqslant C_n^k \leqslant 2^n.$$

Значит, для любого $j = 1, \dots, n$ множество $\{\lambda_j^k \mid k \in \mathbb{N}\}$ конечно, т. е. λ_j — корень из единицы.

8. Существует ли бесконечное множество вещественных квадратных невырожденных матриц, сумма любых двух различных из которых вырождена? *Предложил А. М. Максаев.* (Это основной результат статьи [S. Akbari, M. Jamaali, S.A. Seyed Fakhari, The clique numbers of regular graphs of matrix algebras are finite, Linear Algebra Appl., 431 (2009), 1715-1718].)

Решение. Нет. Пусть $\{A_1, A_2, \dots\}$ — множество матриц $n \times n$, о котором идёт речь. Рассмотрим вещественные многочлены $|A_i + X|$ степени n от n^2 неизвестных элементов матрицы X. Эти многочлены линейно независимы: если $\sum \lambda_i |A_i + X| = 0$ (как многочлен), то для всех j мы имеем $0 = \sum\limits_i \lambda_i |A_i + A_j| = \lambda_j |2A_j|$, то есть $\lambda_j = 0$. Это значит, что число таких многочленов конечно и, стало быть, число матриц A_i конечно.