СЕМНАДЦАТАЯ СТУДЕНЧЕСКАЯ ОЛИМПИАДА ПО АЛГЕБРЕ

Решения

1. Назовём линейное подпространство в пространстве квадратных матриц *невырожденным*, если все содержащиеся в нём матрицы, кроме нулевой, невырождены. Найдите максимальную размерность невырожденного подпространства в пространстве

- а) комплексных $n \times n$ матриц,
- б) вещественных 4×4 матриц,
- в) рациональных $n \times n$ матриц.

Предложил Артём Максимович Макаев

Решение. а) Допустим, что U – невырожденное пространство размерности не менее 2. И пусть A, B – не пропорциональные матрицы из U . Рассмотрим $C = AB^{-1}$. Тогда существует $\lambda \in \mathbb{C}$ такое, что $\det(C - \lambda E) = 0$. Получаем $\det(A - \lambda B) = \det((C - \lambda E)B) = \det(C - \lambda E) \det B = 0$. Противоречие с тем, что $A - \lambda B \in U$.

Одномерным невырожденным пространством является, например, $\{\lambda E \mid \lambda \in \mathbb{C}\}$.

б) Пусть в пространстве матриц $n \times n$ над некоторым полем есть подпространство размерности не менее $n + 1$. Рассмотрим базис этого подпространства $\{A_1, \dots, A_m\}$. Так как $m > n$, первые строки данных матриц линейно зависимы по основной лемме о линейной зависимости. Рассмотрим нетривиальную линейную комбинацию первых строк, равную нулю. В таком случае линейная комбинация матриц с соответствующими коэффициентами будет вырожденной, так как её первая строка нулевая. С другой стороны эта матрица – нетривиальная линейная комбинация базисных, и значит, не нулевая. Значит, данное подпространство не является невырожденным.

Таким образом, невырожденное подпространство в вещественных матрицах 4×4 не может иметь размерность больше 4. Примером невырожденного пространства размерности 4 служит следующее пространство:

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

Несложно видеть, что все строки этой матрицы ортогональны и имеют длину $\sqrt{a^2 + b^2 + c^2 + d^2}$. Значит, если матрица ненулевая, то она невырождена.

в) По доказанному в пункте б) размерность невырожденного подпространства не может быть больше n .

Рассмотрим поле K – расширение $\mathbb{Q}$ степени n . Например, таковым является поле $\mathbb{Q}[x]/(x^n + 2)$. (Многочлен $x^n + 2$ неприводим над $\mathbb{Q}$ по критерию Эйзенштейна.) Выберем в K базис над $\mathbb{Q}$. В рассмотренном примере базисом будет, например, $1, x, \dots, x^{n-1}$. Пусть $h \in K$ – ненулевой элемент. Рассмотрим отображение $\varphi_h: K \rightarrow K$, $\varphi_h(g) = hg$. Ясно, что φ_h – линейный оператор над $\mathbb{Q}$. При этом $\varphi_{h^{-1}} = \varphi_h^{-1}$. Легко видеть, что $\Psi: K \rightarrow \text{GL}(\mathbb{Q}^n)$, $h \mapsto \varphi_h$ – гомоморфизм. Его образ состоит из невырожденных линейных операторов. Если $h \in \text{Ker } \Psi$, то $hg = g$ для всех $g \in K$, что означает $h = 1$. Итак, Ψ – вложение. Следовательно, размерность образа Ψ над $\mathbb{Q}$ равна размерности K , то есть n .

2. Вещественная невырожденная матрица A три на три такова, что $\operatorname{tr}(A^k) = 0$ для бесконечного количества натуральных чисел k . Можно ли утверждать, что A^n – скалярная матрица для некоторого натурального числа n ?

Предложил Антон Александрович Клячко

Решение. Да, можно. Пусть $a, b, c \in \mathbb{C}$ – собственные значения матрицы A . Тогда $u_k = \operatorname{tr}(A^k) = a^k + b^k + c^k$ представляет собой *линейную рекуррентную последовательность*, то есть k -й член (при достаточно больших k) линейно выражается через d предыдущих членов: $u_k = a_1 u_{k-1} + \dots + a_d u_{k-d}$, где d и a_i не зависят от k (в данном случае $d = 3$, а a_i определяются равенством $x^3 - a_1 x^2 - a_2 x - a_3 = (x - a)(x - b)(x - c)$).

Теорема (Теорема Сколема–Малера–Леха¹). *Если $u_1, u_2, \dots$ – линейная рекуррентная последовательность комплексных чисел, то множество её нулей $\{k \in \mathbb{N} \mid u_k = 0\}$ является объединением конечного множества и конечного числа арифметических прогрессий.*

Поскольку в данном случае множество нулей бесконечно, мы имеем арифметическую прогрессию нулей: $a^{l+kj} + b^{l+kj} + c^{l+kj} = 0$ при всех k (и при некоторых фиксированных l и j). Раз матрица вещественная, мы можем считать, что $c \in \mathbb{R}$ и $b = \bar{a}$ (все три собственных значения не могут быть вещественными очевидно). Более того, заменив матрицу A на $\frac{1}{c}A$, мы сведём дело к случаю $c = 1$ и получим, что $a^{l+kj} + \bar{a}^{l+kj} + 1 = 0$. Если a не является корнем из единицы, то это равенство не может выполняться при всех k (упражнение). Значит, $a^n = 1$ и $A^n = E$.

Замечание. Мы признаём, что это решение (и, соответственно, эта задача) несколько выходит за рамки элементарного, которое предполагается на олимпиаде. Фактически мы зачитывали эту задачу, как решённую, тем участникам, которые поняли, что вопрос сводится к такому:

” существуют ли такие вещественные φ и $\varepsilon \notin \{\pm 1, 0\}$, что $2 \cos k\varphi = -\varepsilon^k$ для бесконечного числа целых k ? ”

Решение, представленное выше, фактически принадлежит Жану Абу Самра: <https://mathoverflow.net/q/491724/24165>.

3. Покажите, что произведение $7 \cdot 77 \cdot 777 \cdot 7777 \cdot \dots$ ($n \geq 1$ множителей) никогда не является квадратом целого числа.

Эту задачу мы взяли отсюда <https://mathoverflow.net/q/461766/24165>

Решение. Рассмотрим остаток при делении на 4. У всех множителей, кроме первого, он равен 1, а у первого 3. Значит, остаток при делении на 4 всего произведения равен 3. Однако, квадрат не может иметь остаток 3 при делении на 4.

4. Покажите, что многочлен $f(x) + i$ имеет простой (т.е. кратности один) корень в $\mathbb{C}$, если $f(x) \in \mathbb{R}[x]$ и не константа.

Эту задачу мы взяли отсюда <https://mathoverflow.net/q/473887/24165>

Решение. Заметим, что если $g(x) = f(x) + i$ имеет корень z , то $\bar{z}$ – не корень g . В самом деле $g(\bar{z}) = f(\bar{z}) + i = \overline{f(z)} + i = \overline{-i} + i = 2i$. Кратные корни g – это общие корни g и $g' = f'$. При этом каждый корень g' имеет сопряжённый корень той же кратности. Значит, $\deg \gcd(g, g') \leq \frac{\deg g'}{2} < \frac{\deg g}{2}$. С другой стороны, предположим, что все корни g являются кратными. Тогда их кратности в $\gcd(g, g')$ на 1 меньше. Значит

¹см., например, А. Я. Канель-Белов, Задачи о линейных рекуррентах, Мат. просвещение, сер. 3, 30 (2023), 192-208, <https://www.mathnet.ru/mp1074>

корень кратности m в g даёт вклад в степень $\gcd(g, g')$ равный $m - 1 \geq \frac{m}{2}$. Отсюда $\deg \gcd(g, g') \geq \frac{\deg g}{2}$. Противоречие.

5. Покажите, что если множество всех квадратов элементов поля является собственным подполем, то характеристика поля равна двум.

Предложил Антон Александрович Клячко

Решение. Допустим, что в поле F характеристики не 2 квадраты образуют подполе $K \subsetneq F$. Тогда существует $x \in F \setminus K$. Имеем $1 = 1^2 \in K$, а значит, $2 = 1 + 1 \in K$. Так как характеристика F не 2, получаем $2 \neq 0$. При этом $(x + 1)^2 - x^2 - 1^2 = 2x \in K$. Так как $2x \in K$ и $2 \in K$ – ненулевой элемент, их частное $x = \frac{2x}{2} = x \in K$. Противоречие.

6. Покажите, что автоморфизм порядка два неединичной абелевой группы всегда имеет неединичную инвариантную циклическую подгруппу.

Предложил Антон Александрович Клячко

Решение. Рассмотрим ненулевой элемент a . Пусть φ – автоморфизм из условия. Тогда если $\varphi(a) = a$, то $\varphi(\langle a \rangle) = \langle a \rangle$. Иначе $\varphi(a) = b \neq a$. Тогда $\varphi(b - a) = \varphi(b) - \varphi(a) = \varphi^2(a) - b = a - b$. Значит, $\varphi(\langle a - b \rangle) = \langle a - b \rangle$.

7. Покажите, что в каждой конечной неразрешимой группе найдётся подгруппа, не изоморфная никакой нормальной подгруппе.

Эту задачу мы взяли отсюда <https://mathoverflow.net/q/370056/24165>

Решение.

Пусть G – данная группа и $|G| = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ – разложение на простые множители. Пусть $H_1, \dots, H_k$ – силовские подгруппы, то есть $|G_i| = p_i^{\alpha_i}$. Если для каждого i подгруппа H_i нормальна, то $G = H_1 \times \dots \times H_k$. (Стандартное упражнение.) Однако поскольку каждая H_i разрешима, то и G разрешима. Значит, существует H_j , не являющаяся нормальной. Однако, любая подгруппа H , изоморфная H_j имеет $p_j^{\alpha_j}$ элементов, следовательно, она также силовская и сопряжена H_j . То есть H не нормальна.

8. Покажите, что над полем из двух элементов конечная абелева группа обладает неприводимым

- а) двумерным представлением тогда и только тогда, когда её порядок делится на 3,
- б) четырёхмерным представлением тогда и только тогда, когда её порядок делится на 5.

Предложил Антон Александрович Клячко

Решение. а) Группа $\mathrm{GL}_2(\mathbb{F}_2)$ содержит 6 элементов и не является абелевой, так как

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Значит, $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$. Если порядок группы G не делится на 3, то для любого гомоморфизма $\rho: G \rightarrow \mathrm{GL}_2(\mathbb{F}_2)$, образ не содержит элементов порядка 3. Значит, либо

$$\mathrm{Im} \rho = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\},$$

либо $\mathrm{Im} \rho \cong \mathbb{Z}_2$. В любом случае представление ρ не может быть неприводимым.

Если же $|G|$ делится на 3, поскольку G – абелева группа, существует гомоморфизм $G: \mathbb{Z}_3$. Осталось показать, что существует неприводимое двумерное представление

группы $\mathbb{Z}_3$ над $\mathbb{F}_2$. Рассмотрим такое представление ρ :

$$\rho(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho(1) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \rho(2) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Несложно видеть, что оно неприводимо. (Заметим, что данное представление получается из разложения трёхмерного мономиального представления $\mathbb{Z}_3$ на неприводимые.)

б) Если $|G|$ делится на 5, поскольку G – абелева группа, существует гомоморфизм $G: \mathbb{Z}_5$. Предъявим неприводимое четырёхмерное представление группы $\mathbb{Z}_5$ над $\mathbb{F}_2$. Рассмотрим такое представление ρ :

$$\rho(0) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \rho(1) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad \rho(2) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix},$$

$$\rho(3) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \quad \rho(4) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Покажем, что данное представление неприводимо. Так как $\text{char } \mathbb{F}_2 = 2 \nmid 5$, применима теорема Машке. Значит, если представление приводимо, то существует 1-мерное или 2-мерное инвариантное подпространство. Несложно видеть, что ненулевого неподвижного вектора нет, а значит, нет 1-мерного инвариантного подпространства. Если же есть 2-мерное инвариантное подпространство, но нет 1-мерного, то получаем неприводимое 2-мерное представление группы $\mathbb{Z}_5$ над полем $\mathbb{F}_2$. Однако, как было установлено в пункте а), $\text{GL}_2(\mathbb{F}_2) \cong S_3$. Следовательно, любой гомоморфизм $\mathbb{Z}_5 \rightarrow \text{GL}_2(\mathbb{F}_2)$ тривиален.

Теперь покажем, что условие, что $|G|$ делится на 5 необходимо для того, чтобы существовало неприводимое представление $\rho: G \rightarrow \text{GL}(\mathbb{F}_2^4)$. Имеем

$$|\text{GL}_4(\mathbb{F}_2)| = (2^4 - 1)(2^4 - 2)(2^4 - 4)(2^4 - 8) = 15 \cdot 14 \cdot 12 \cdot 8 = 2^6 \cdot 3^2 \cdot 5 \cdot 7.$$

Так как G абелева, её образ при ρ также абелев. Значит, если оператор φ лежит в образе ρ , то множество неподвижных относительно φ векторов является инвариантным подпространством (относительно всего образа ρ). Заметим, что

$$|\text{GL}_3(\mathbb{F}_2)| = (2^3 - 1)(2^3 - 2)(2^3 - 4) = 2^3 \cdot 3 \cdot 7.$$

Значит, в $|\text{GL}_3(\mathbb{F}_2)|$ есть элемент порядка 7. Так как циклическая группа порядка 7 в $\text{GL}_4(\mathbb{F}_2)$ является силовской, любой элемент порядка 7 из $\text{GL}_4(\mathbb{F}_2)$ сопряжён элементу из $\text{GL}_3(\mathbb{F}_2)$, то есть имеет неподвижный вектор. По сказанному выше это противоречит неприводимости ρ . Значит, в образе ρ нет элемента порядка 7.

Если в образе ρ есть элемент порядка 2^k , то там есть элемент порядка 2. Пусть это ψ . Рассмотрим любой ненулевой вектор u . Положим $v = \psi(u)$. Если $v = u$, то мы нашли неподвижный относительно ψ ненулевой вектор, что противоречит неприводимости ρ . Если же $v \neq u$, то $u + v$ – неподвижный относительно ψ вектор. Итак, в образе ψ нет элементов порядка 2^k .

Если образ ρ содержит элемент порядка 5, то порядок образа ρ делится на 5, а значит, порядок G также делится на 5. Пусть это не так. Тогда в образе ρ лежат только элементы порядка 3^k . Но тогда $\rho(G)$ содержится в силовской 3-подгруппе группы

$GL_4(\mathbb{F}_2)$. Однако, силовскую 3-подгруппу группы $GL_4(\mathbb{F}_2)$ можно предъявить: она состоит из матриц вида

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

где A и B (независимо) пробегает множество

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Данное множество матриц даёт приводимое представление. Так как все силовские 3-подгруппы сопряжены, представление ρ приводимо, что даёт противоречие.