ШЕСТНАДЦАТАЯ СТУДЕНЧЕСКАЯ ОЛИМПИАДА ПО АЛГЕБРЕ НА МЕХМАТЕ МГУ. РЕШЕНИЕ НЕКОТОРЫХ ЗАДАЧ

1. Линейный оператор на пространстве $n \times n$ матриц переводит каждую невырожденную матрицу в матрицу с тем же определителем. Докажите, что он также переводит каждую вырожденную матрицу в вырожденную.
Предложил А. М. Максаев.

Ответ. Это верно тогда и только тогда, когда поле состоит больше, чем из двух элементов. (На самом деле подразумевалось, что задача над полем вещественных чисел, об этом мы сказали устно на олимпиаде.)

Решение. Пусть матрица A вырожденная, а $\varphi\colon \mathrm{M}_n(F) \to \mathrm{M}_n(F)$ — линейное отображение, сохраняющее определитель невырожденных матриц.

$$|\varphi(A - xE)| = |A - xE|, \quad \text{если } |A - xE| \text{ не ноль.}$$

И левая, и правая часть этого равенства суть многочлены от x (левая из-за линейности отображения φ).

Если поле F бесконечно, то эти многочлены равны в бесконечном числе точек. Стало быть, они равны как многочлены, то есть их значения равны и при нулевом x, что и требовалось.

Для конечного поля такое рассуждение не работает; однако в этом случае

достаточно показать, что оператор φ невырожден (= биективен).

Пусть $\ker\varphi \ni A \neq 0$. Матрица A обязана быть вырожденной, поскольку оператор φ сохраняет определители невырожденных матриц.

Упражнение 1. Квадратные матрицы A и B имеют одинаковые ранги и определители тогда и только тогда, когда $A = SBT$ для некоторых матриц S и T таких, что $|ST| = 1$.

Это упражнение показывает, что матрицу A можно считать диагональной:

$$A = \mathrm{diag}(1, \ldots, 1, 0, \ldots, 0), \quad \text{где } k > 0 \text{ единиц и } n - k \text{ нулей}$$

(поскольку оператор $X \mapsto \varphi(SXT)$ при $|ST| = 1$ тоже сохраняет определители невырожденных матриц и его биективность равносильна биективности оператора φ). Возьмём теперь матрицу $C = \mathrm{diag}\left(D, \underbrace{1, \ldots, 1}_{n-k \text{ штук}}\right)$, где D — матрица размера $k \times k$ с характеристическим многочленом $(-1)^k x^k + \delta$. Здесь мы пользуемся тем, что существует матрица с любым наперёд заданным характеристическим многочленом (с правильным старшим коэффициентом).

Упражнение 2. Напишите в явном виде такую матрицу D.

Теперь выберем $\delta \in F$ так, чтобы $\delta \neq 0 \neq (-1)^k + \delta$ (это возможно, если $|F| > 2$). Тогда матрицы C и $C - A$ невырожденные, с разными определителями: $|C| = \delta \neq (-1)^k + \delta = |C - A|$, но $\varphi(C - A) = \varphi(C) - \varphi(A) = \varphi(C)$, то есть оператор φ не у всех невырожденных матриц сохраняет определители. Это противоречие завершает доказательство в случае $|F| > 2$.

Если же $F = \mathbb{Z}_2$, то утверждение неверно. Вот пример такого экзотического оператора:

$$\varphi\colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} b+d & b \\ b & d \end{pmatrix}.$$

(Определитель правой матрицы — это $b^2 + d^2 + bd = b + d + bd$, что обращается в ноль только при $b = d = 0$.)

2. В своем докладе аспирант рассмотрел некоторую подгруппу G аддитивной группы комплексных $n\times n$ матриц $\mathrm{M}_n(\mathbb{C})$ и заявил, что (комплексная) линейная оболочка G совпадает с $\mathrm{M}_n(\mathbb{C})$. Присутствующий в аудитории профессор прослушал точное определение G, но тотчас же отметил, что в ней обязана содержаться невырожденная матрица. Как ему удалось это понять?
Предложил А. М. Максаев.

Решение. Рассмотрим $k = n^2$ линейно независимых матриц $A_1, \ldots, A_k \in G$ и многочлен $f(x_1, \ldots, x_k) = \det\left(\sum x_j A_j\right) \in \mathbb{C}[x_1, \ldots, x_k]$. Этот многочлен ненулевой (поскольку

$$\left\{\sum x_j A_j \mid x_j \in \mathbb{C}\right\} = \mathrm{M}_n(\mathbb{C})$$

по условию). Осталось установить следующий факт:

ненулевой многочлен $f \in \mathbb{C}[x_1, \ldots, x_k]$ принимает ненулевое значение при некоторых целых значениях переменных.

Доказательство состоит в индукции по k. Пусть $f(x_1, \ldots, x_k) = f_0 + f_1 x_k + \ldots + f_m x_k^m$. Так как $f \neq 0$, один из многочленов многочлен $f_j \in \mathbb{C}[x_1, \ldots, x_{k-1}]$ ненулевой. Тогда по предположению индукции $f_j(a_1, \ldots, a_{k-1}) \neq 0$ при некоторых целых a_i. Значит, многочлен $f(a_1, \ldots, a_{k-1}, x_k) \in \mathbb{C}[x_k]$ ненулевой и, следовательно он принимает ненулевое значение в некоторой целой точке a_k (поскольку по теореме Безу число корней ненулевого многочлена от одной переменной конечно). Значит, набор $(a_1, \ldots, a_{k-1}, a_k) \in \mathbb{Z}^k$ искомый.

3. Пусть A и B — вещественные матрицы 5×7, строки матрицы A ортогональны строкам матрицы B (относительно стандартного скалярного произведения в $\mathbb{R}^7$), а столбцы матрицы A ортогональны столбцам матрицы B. Можно ли утверждать, что
$\operatorname{rank}(A + B) = \operatorname{rank} A + \operatorname{rank} B$?
Эту задачу мы позаимствовали в статье: `https://doi.org/10.4153/CMB-1972-082-8` .
Там же есть решение.

4. Покажите, что если $A^{2025} = E$, где A — вещественная матрица сто на сто, то $\chi_A(1) \geqslant 0$, где χ_A — характеристический многочлен матрицы A.
Эту задачу мы позаимствовали здесь: `https://mathoverflow.net/q/370782/24165` .
Там же есть решение.

5. Для каких конечных групп G комплексная групповая алгебра $\mathbb{C}[G]$ порождается одним элементом?
Предложили А. Э. Гутерман, А. А. Клячко, О. В. Маркова и М. А. Хрыстик.

Решение. Для всех абелевых и только для них.

Если групповая алгебра порождается одним элементом, то она коммутативна, и, следовательно, группа обязана быть абелевой. В другую сторону так: если группа G конечна и абелева, то групповая алгебра, как известно, изоморфна прямой сумме $|G|$ экземпляров поля $\mathbb{C}$ (изоморфизм $\mathbb{C}[G] \to \mathbb{C}\oplus\ldots\oplus\mathbb{C}$ такой: $g \mapsto \big(\varphi_1(g), \varphi_2(g), \ldots\big)$, где $\varphi_k\colon G \to \mathbb{C}^*$ — неприводимые (одномерные) представления группы G). Прямая сумма $\mathbb{C}\oplus\ldots\oplus\mathbb{C}$ очевидно порождается (например) элементом $(1, 2, 3, \ldots)$, поскольку для любых комплексных чисел $b_1, \ldots, b_n$ найдётся такой многочлен $f \in \mathbb{C}[x]$, что $f(1) = b_1, \ldots, f(n) = b_n$.

Более тонкие вещи на эту тему можно найти здесь:

[GMKh22] A. Guterman, O. Markova, M. Khrystik, On the lengths of group algebras of finite abelian groups in the semi-simple case, Journal of Algebra and Its Applications, 21:07, 2250140 (https://doi.org/10.1142/S0219498822501407).

6. Покажите, что в конечной группе, удовлетворяющей тождеству $x^6 = 1$, число элементов порядка шесть сравнимо с нулём или двойкой по модулю шесть.
Эту задачу мы позаимствовали здесь: `https://mathoverflow.net/q/383624/24165`.

Решение. Если элементов порядка три нет, то, очевидно, нет и элементов порядка шесть, так что в этом случае доказывать нечего.

Рассмотрим теперь действие сопряжением подгруппы H порядка три на множестве циклических подгрупп порядка шесть. Длина каждой орбиты равна либо тройке, либо единице. В циклической группе порядка шесть есть ровно два элемента порядка шесть. Поэтому, число элементов порядка шесть, лежащих в циклических подгруппах порядка шесть, не нормализуемых подгруппой H делится на шесть.

Осталось понять, сколько элементов порядка шесть в циклических подгруппах порядка шесть, нормализуемых подгруппой H. Все эти элементы, на самом деле, коммутируют с H, поскольку циклическая группа порядка шесть не имеет автоморфизмов порядка три.

Таким образом, очевидная индукция по порядку группы сводит задача к следующей:

> в конечной группе G с тождеством $x^6 = 1$ все элементы порядка три коммутируют со всеми элементами порядка шесть; надо показать, что число элементов порядка шесть сравнимо с нулём или двойкой по модулю шесть.

Можно, очевидно, считать, что
- группа порождается элементами порядка шесть;
- следовательно, все элементы порядка три центральные;
- значит, силовская 3-подгруппа центральная (так как все её неединичные элементы имеют порядок три);
- а силовская 2-подгруппа абелева (поскольку удовлетворяет тождеству $x^2 = 1$);
- но группа G является произведением силовской 2-подгруппы и силовской 3-подгруппы (так как пересечение этих подгрупп тривиально, а произведение порядков равно $|G|$);
- стало быть, $G \simeq \mathbb{Z}_3 \oplus \ldots \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \ldots \oplus \mathbb{Z}_2$.

И тогда

$$\begin{aligned}(\text{число элементов порядка } 6) =&(\text{число элементов порядка } 3) \cdot (\text{число элементов порядка } 2) = \\ =&(3^n - 1) \cdot (2^m - 1) \equiv 2 \cdot (3 \text{ или } 1) \pmod 6.\end{aligned}$$

7. Назовём кольцо R *безушным*, если число корней в R каждого многочлена из $R[x]$ ненулевого не превосходит его степени. При каких n кольцо вычетов $\mathbb{Z}_n$ безушно?
Предложил А. А. Клячко.

Решение. При простых n и только при простых.

Если n простое, то $\mathbb{Z}_n$ поле, поэтому теорема Безу выполняется. Если же $n = kl$ не простое, то линейный многочлен kx имеет $k > 1$ корней.

Упражнение. При каких n число корней всякого многочлена $f \in \mathbb{Z}_n[x]$ со старшим коэффициентом 1 не превосходить степени многочлена f?

8. Верно ли, что в векторном пространстве $\mathbb{Q}[x]$ операторы $h \mapsto hf$ и $h \mapsto hg$, где f и g — фиксированные многочлены положительной степени, подобны тогда и только тогда, когда $\deg f = \deg g$?
Предложил А. А. Клячко.

Решение. Да, верно. Пусть многочлен f имеет степень n. Рассмотрим в пространстве $\mathbb{Q}[x]$ базис

$$1, x, x^2, \ldots, x^{n-1}, f, xf, x^2f, \ldots, x^{n-1}f, f^2, xf^2, \ldots \quad \text{(Ясно, что это базис?)}$$

Оператор S' сдвига координат в этом базисе, переводящий каждый базисный вектор в следующий, подобен оператору S умножения на x, поскольку оператор S действует сдвигом координат в стандартном базисе $1, x, x^2, \ldots$. Следовательно, оператор $(S')^n$ подобен оператору S^n. Осталось заметить, что $S'(h) = fh$ и $S(h) = x^n h$ для всех $h \in \mathbb{Q}[x]$.