Решения задач шестой студенческой олимпиады по алгебре

Задача 1

Докажите, что если все элементы действительной квадратной матрицы порядка больше двух отличны от нуля, то их можно умножить на положительные числа так, чтобы матрица стала вырожденной. (*Олимпиада мехмата 1980 г.*)

Решение 1. Рассмотрим один столбец матрицы. Допустим, что в нём есть и положительные и отрицательные числа. Пусть сумма чисел в этом столбце равна $S \neq 0$. Выберем элемент x данного столбца, противоположный S по знаку. Тогда, умножив x на подходящее положительное число, мы можем добиться того, что сумма чисел в этом столбце будет равна нулю. Таким образом, если в каждом столбце есть числа обоих знаков, то можно умножить по одному числу из каждого столбца на положительное число так, чтобы сумма строк стала равна нулю, а значит, матрица стала вырожденной.

Допустим, что A — матрица $n \times n$, удовлетворяющая условиям задачи, элементы которой нельзя умножить на положительные числа так, чтобы она стала вырожденной. Тогда в A есть столбец, все элементы которого одного знака. Обозначим номер одного из таких столбцов через k. Рассмотрим матрицы $A_1, \ldots, A_n$, где A_i получена из матрицы A умножением i-й строки на -1. Докажем, что существует такой номер $1 \leqslant j \leqslant n$, что в каждом столбце матрицы A_j есть элементы обоих знаков. Действительно, пусть для каждого $1 \leqslant i \leqslant n$ в матрице A_i есть столбец с номером $\varphi(i)$, все элементы которого одного знака. Однако, из того, что $n \geqslant 3$, следует, что все числа $\varphi(1), \ldots, \varphi(n), k$ различны, чего не может быть.

Итак, в каждом столбце матрицы A_j есть числа обоих знаков. Значит, по доказаному ранее, элементы A_j можно умножить на такие положительные числа, что получившаяся матрица B_j будет вырожденой. Умножим элементы матрицы A на те же числа, получим матрицу B. Заметим, что матрица B получается из B_j умножением j-й строки на -1. Таким образом, ранги у матриц B и B_j совпадают. А значит, матрица B вырождена.

Решение 2. В развёрнутой формуле определителя матрицы порядка $n \geqslant 3$ встречаются как положительные, так и отрицательные слагаемые (докажите!). Предположим не теряя общности, что определитель нашей матрицы положителен. Рассмотрим тогда наибольшее по модулю отрицательное слагаемое S. Умножим все входящие в него элементы матрицы на x. Тогда новый определитель будет многочленом от x степени n, причем коэффициентом при x^n будет именно S. При достаточно большом x определитель станет отрицательным (докажите этот факт!), а при $x = 1$ он положителен. Так как многочлен — непрерывная функция, то при некотором положительном x он равен 0.

Упражнение. Будет ли утверждение верным, если ровно один из элементов матрицы равен нулю?

Задача 2

Покажите, что вещественная матрица A размера 2011×2011 вырождена тогда и только тогда, когда её можно превратить в $-A$ элементарными преобразованиями вида *прибавление к одной строке другой, умноженной на число.* (*Предложил А. А. Клячко.*)

Решение. При элементарных преобразованиях такого типа сохраняется определитель, поэтому невырожденная матрица A не может быть превращена в $-A$, так как $|-A| = (-1)^{2011}|A| = -|A| \neq |A|$, если $|A| \neq 0$.

Допустим теперь, что матрица A вырождена. Тогда, как известно, она может быть превращена в матрицу A' с нулевой строкой при помощи нескольких преобразований $T_1, \ldots, T_k$ указанного типа: $A' = T_k \circ \ldots \circ T_1(A)$. Матрицу A' с нулевой последней строкой легко превратить в $-A'$. Действительно, для всех i от единицы до 2010 достаточно проделать следующие преобразования:

U_i: прибавление i-й строки к последней;

V_i: вычитание из i-й строки удвоенной последней;
U_i: ещё одно прибавление i-й строки к последней.

Теперь ясно, что

$$-A = T_1^{-1} \circ \cdots \circ T_k^{-1}(-A') =$$
$$= T_1^{-1} \circ \cdots \circ T_k^{-1} \circ U_1 \circ V_1 \circ U_1 \circ \cdots \circ U_{2010} \circ V_{2010} \circ U_{2010}(A') =$$
$$= T_1^{-1} \circ \cdots \circ T_k^{-1} \circ U_1 \circ V_1 \circ U_1 \circ \cdots \circ U_{2010} \circ V_{2010} \circ U_{2010} \circ T_k \circ \cdots \circ T_1(A)$$

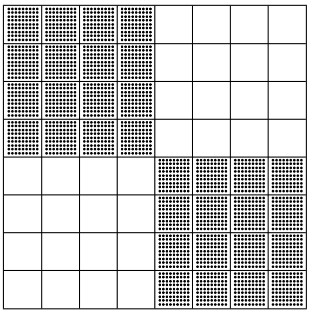
Упражнение. Покажите, что любая матрица 2012×2012 может быть превращена в минус себя преобразованиями указанного типа. Найдите наименьшее число преобразований, необходимых для превращения единичной матрицы в минус единичную.

Задача 3

Какие бы вещественные числа Змей Горыныч ни написал на чёрных клетках шахматной доски, Иванушка-дурачок может заполнить белые клетки так, что получится матрица ранга r. Для каких r это возможно? (*Предложил А. А. Клячко.*)

Ответ. 4, 5, 6, 7 и 8.

Решение. Перестановками строк и столбцов шахматная доска приводится к виду



На такой упрощённой шахматной доске ясно видно, что сделать ранг 0, 1, 2 или 3 Иванушка не сможет (если Змей ему не подыграет), так как Змей полностью контролирует минор порядка четыре и сможет сделать его ненулевым, если захочет.

Докажем теперь, что любой ранг больший трёх Иванушка сделать сможет, как бы Горыныч ни старался ему помешать. Другими словами, Иванушка должен для любого числа $r \in \{4, 5, 6, 7, 8\}$ и любых матриц Z и G размера 4×4 подбирать матрицы I и D размера 4×4 такие, что $\operatorname{rk}\begin{pmatrix} Z & I \\ D & G \end{pmatrix} = r$. Решением задачи будет, например, следующая пара матриц: $I = E$ и $D = X + GZ$, где X — любая матрица 4×4 ранга $r - 4$. Действительно,

$$\operatorname{rk}\begin{pmatrix} Z & E \\ X + GZ & G \end{pmatrix} = \operatorname{rk}\left(\begin{pmatrix} Z & E \\ X + GZ & G \end{pmatrix}\begin{pmatrix} E & 0 \\ -Z & E \end{pmatrix}\right) = \operatorname{rk}\begin{pmatrix} 0 & E \\ X & G \end{pmatrix} =$$
$$= \operatorname{rk}\left(\begin{pmatrix} E & 0 \\ -G & E \end{pmatrix}\begin{pmatrix} 0 & E \\ X & G \end{pmatrix}\right) = \operatorname{rk}\begin{pmatrix} 0 & E \\ X & 0 \end{pmatrix} = 4 + \operatorname{rk} X = r.$$

Мы воспользовались тем, что умножение слева и справа на невырожденные матрицы не меняет ранг.

Упражнение. Как изменится ответ, если Иванушка контролирует только одну большую диагональ шахматной доски, а Горыныч — всё остальное?

Задача 4

Покажите, что каждый многочлен от одной переменной с комплексными коэффициентами, отображающий все корни из единицы в корни из единицы, является одночленом. (*Предложил А. А. Клячко.*)

Решение. Если многочлен $f(x) = \sum a_k x^k$ отображает корни из единицы в корни из единицы, то $f(a)\overline{f}(\overline{a}) = 1$ для любого корня из единицы a, где $\overline{f}(x) = \sum \overline{a_k} x^k$ — сопряжённый многочлен. При этом $\overline{a} = \frac{1}{a}$, то есть многочлен Лорана $g(x) = f(x)\overline{f}(\frac{1}{x}) - 1$ имеет бесконечно много корней (все корни из единицы являются его корнями). Значит, $g(x)$ является константой, то есть

$$f(x)\overline{f}\left(\frac{1}{x}\right) = \mathrm{const}\,.$$

Это возможно только, если f является одночленом, так как при умножении многочленов Лорана максимальные степени их членов складываются и минимальные степени их членов тоже складываются:

$$\left(b_p x^p + b_{p+1}x^{p+1} + \dots + b_P x^P\right)\left(c_q x^q + b_{q+1}x^{q+1} + \dots + c_Q x^Q\right) = b_p c_q x^{p+q} + \dots + b_P c_Q x^{P+Q}.$$

Упражнение 1. Верно ли, что рациональная дробь над полем комплексных чисел, принимающая вещественные значения во всех вещественных точках, в которых её значение определено, равна дроби с вещественными коэффициентами?

Задача 5

Покажите, что разрешимая группа, в которой коммутант выделяется прямым сомножителем, абелева. (*Предложил В. Шмаров.*)

Решение. Коммутант прямого произведения групп есть прямое произведение их коммутантов (докажите!). Поэтому, если $G = G' \times A$, то $A' = \{1\}$ и $G' = G''$. Первое из этих равенств означает, что группа A абелева, а второе означает, что $G' = G'' = G''' = \dots = \{1\}$ в силу разрешимости.

Упражнение. Покажите, что центр прямого произведения групп есть прямое произведение их центров. Докажите аналогичное разложение для каждого класса сопряжённости прямого произведения групп. Верно ли, что каждый идеал прямой суммы колец есть прямая сумма некоторых идеалов слагаемых?

Задача 6

Пусть $\mathbb{K}$ — поле нулевой характеристики и $\mathbb{L}_1, \dots, \mathbb{L}_n$ — набор его конечных расширений. Докажите, что $\mathbb{L}_1 \oplus \dots \oplus \mathbb{L}_n$ порождается над $\mathbb{K}$ одним элементом (то есть найдётся такой элемент h этой алгебры, что все остальные элементы выражаются как многочлены от h с коэффициентами из $\mathbb{K}$). (*Предложил А. В. Гришин.*)

Решение. *Шаг 1.* Докажем, что каждое конечное расширение $\mathbb{L}$ поля $\mathbb{K}$ порождается над $\mathbb{K}$ одним элементом (теорема о примитивном элементе). Здесь мы следует изложению из параграфа 46 книги (Б. Л. ван дер Варден. Алгебра. М.: Наука, 1976).

Используя индукцию, достаточно доказать утверждение в случае, когда расширение $\mathbb{L}$ порождается двумя элементами, т.е. $\mathbb{L} = \mathbb{K}(\alpha, \beta)$. Пусть $f(x)$ и $g(x)$ – минимальные многочлены элементов α и β над полем $\mathbb{K}$ и $\mathbb{F}$ – конечное расширение поля $\mathbb{K}$, в котором многочлены $f(x)$ и $g(x)$ разлагаются на линейные множители. Пусть $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m$ и $\beta_1 = \beta, \beta_2, \dots, \beta_k$ – корни этих многочленов в поле $\mathbb{F}$. Из неприводимости многочленов $f(x)$ и $g(x)$ над $\mathbb{K}$ следует, что эти корни являются попарно различными элементами поля $\mathbb{F}$. Поскольку поле $\mathbb{K}$ бесконечно, найдется такой элемент $c \in \mathbb{K}$, что $\alpha_i + c\beta_j \neq \alpha_1 + c\beta_1$ при всех $i, j \neq 1$. Покажем, что $\mathbb{L} = \mathbb{K}(\theta)$, где $\theta = \alpha + c\beta$.

Элемент β удовлетворяет уравнениям $g(x) = 0$ и $f(\theta - cx) = 0$, коэффициенты которых лежат в $\mathbb{K}(\theta)$. Многочлены $g(x)$ и $f(\theta - cx)$ имеют лишь один общий корень, поскольку для остальных корней β_j многочлена $g(x)$ имеем $\theta - c\beta_j \neq \alpha_i$. Значит, многочлены $g(x)$ и $f(\theta - cx)$ имеют лишь один общий линейный множитель $x - \beta$. Коэффициенты этого множителя лежат в $\mathbb{K}(\theta)$. Значит, β и $\alpha = \theta - c\beta$ лежат в $\mathbb{K}(\theta)$, и $\mathbb{L} = \mathbb{K}(\theta)$. [1]

Далее мы используем подход из главы 11 книги (Э. Б. Винберг. Курс алгебры. М.: Факториал Пресс 2002).

Шаг 2. Пусть A – алгебра над полем $\mathbb{K}$ и $\mathbb{F}$ – некоторое расширение поля $\mathbb{K}$. Векторное пространство $A(\mathbb{F}) := A \otimes_{\mathbb{K}} \mathbb{F}$, снабженное умножением

$$(\lambda \otimes u)(\mu \otimes v) = \lambda\mu \otimes uv,$$

является алгеброй над полем $\mathbb{F}$. Ясно, что если $A = A_1 \oplus A_2$ – прямая сумма алгебр, то $A(\mathbb{F}) = A_1(\mathbb{F}) \oplus A_2(\mathbb{F})$. Далее, если $A = \mathbb{K}(\alpha)$ – простое расширение поля $\mathbb{K}$, рассматриваемое как алгебра над $\mathbb{K}$, и $f(x)$ – минимальный многочлен элемента α над $\mathbb{K}$, то $A \cong \mathbb{K}[x]/(f(x))$. Если над полем $\mathbb{F}$ многочлен $f(x)$ разлагается на линейные множители, то

$$A(\mathbb{F}) \cong \mathbb{F}[x]/(f(x)) \cong \mathbb{F} \oplus \ldots \oplus \mathbb{F} \quad (m \text{ копий}),$$

где m – степень многочлена $f(x)$.

Шаг 3. Пусть A – алгебра конечной размерности s над полем $\mathbb{K}$. Покажем, что если для некоторого расширения $\mathbb{F}$ поля $\mathbb{K}$ алгебра $A(\mathbb{F})$ порождается над полем $\mathbb{F}$ одним элементом, то и алгебра A порождается над $\mathbb{K}$ одним элементом. Если это не так, то для любого $a \in A$ элементы $1, a, \ldots, a^{s-1}$ линейно зависимы над $\mathbb{K}$. Это можно записать в виде тождественного равенства нулю определителя, составленного из координат элементов $1, a, \ldots, a^{s-1}$ в некотором базисе пространства A. Как функция от координат элемента a этот определитель представляет собой некоторый многочлен с коэффициентами из $\mathbb{K}$. Если он равен нулю при всех значениях переменных в поле $\mathbb{K}$, то он является нулевым многочленом, и, следовательно, равен нулю и при всех значениях переменных в расширении $\mathbb{F}$ поля $\mathbb{K}$. Значит, алгебра $A(\mathbb{F})$ не порождается над полем $\mathbb{F}$ одним элементом, противоречие.

Шаг 4. Вернемся к алгебре $A = \mathbb{L}_1 \oplus \ldots \oplus \mathbb{L}_n$ из условия задачи. Как следует из доказанного выше, найдется такое конечное расширение $\mathbb{F}$ поля $\mathbb{K}$, что $A(\mathbb{F}) \cong \mathbb{F} \oplus \ldots \oplus \mathbb{F}$ (r копий) для некоторого натурального r. Достаточно доказать, что эта алгебра порождается над $\mathbb{F}$ одним элементом. Рассмотрим элемент $c = (c_1, \ldots, c_r)$, где все компоненты $c_i \in \mathbb{F}$ попарно различны. Тогда определитель, составленный из координат элементов $1, c, \ldots, c^{r-1}$, есть определитель Вандермонда для $c_1, \ldots, c_r$ и, значит, отличен о нуля.

Замечание. В качестве альтернативы шагам 2–4 можно показать, что у порождающих элементов полей $\mathbb{L}_i$ минимальные многочлены f_i можно считать попарно непропорциональными. После этого набор из этих порождающих элементов будет порождать подалгебру, изоморфную $K[x]/(f_1, \ldots, f_n)$, и из соображений размерности она совпадет со всей алгеброй.

Задача 7

Покажите, что простая группа не может содержать подгрупп двух разных простых индексов. (*Предложил Е. П. Вдовин.*)

Решение. Пусть G — простая группа и предположим, что она содержит подгруппы различных простых индексов p и q. Без ограничения общности можно считать, что $p < q$. Пусть H — подгруппа группы G индекса p. Рассмотрим действие группы G на правых смежных классах $\{Hx \mid x \in G\}$ правыми умножениями. Это действие даёт гомоморфизм φ из G в симметрическую группу S_p степени p. Поскольку $H \neq G$, образ группы G относительно построенного гомоморфизм нетривиален. Так как группа G проста, получаем, что образ $\varphi(G)$ изоморфен группе G (в частности, группа G конечна). Но q с одной стороны делит $|G|$, а с другой — не делит $|S_p|$, значит, не делит $|\varphi(G)| = |G|$, противоречие.

[1] Отметим, что теорема о примитивном элемента не всегда верна над полями положительной характеристики. Например, можно рассмотреть конечное расширение $\mathbb{Z}_p(x^p, y^p) \subset \mathbb{Z}_p(x, y)$.

Упражнение 1. Покажите, что если простая группа содержит подгруппу простого индекса p, то p — наибольший простой делитель порядка группы и p^2 не делит порядок группы.

Задача 8

Покажите, что произведение любых пяти комплексных матриц 3×3 можно представить как линейную комбинацию произведений менее пяти сомножителей, каждый из которых равен одной из этих пяти матриц. (Произведение нуля сомножителей считается единичной матрицей.) Решите аналогичную задачу для матриц 2×2. На какое наименьшее число можно заменить пять в этом случае? (*Предложили А. Э. Гутерман и О. В. Маркова.*)

Решение 1. Пусть имеется пять матриц 3×3: A, B, C, D и F. Рассмотрим все конечные последовательности, составленные из этих матриц, и упорядочим эти последовательности по длине, а при равной длине — по алфавиту:

$$\text{пустая последовательность } < (A) < (B) < (C) < (D) < (F) < (A, A) < (A, B) < \dots$$

Будем говорить, что последовательность *сократима*, если произведение её элементов линейно выражается через произведения элементов меньших (в этом смысле) последовательностей. (Произведение элементов пустой последовательности считается, как всегда, единичной матрицей.)

Предположим, что существует последовательность длины пять, произведение элементов которой не выражается через произведения элементов последовательностей меньшей длины. Минимальная (в смысле введённого порядка) такая последовательность, очевидно, несократима. Поэтому, чтобы получить противоречие, достаточно доказать, что каждая последовательность $(X_1, X_2, X_3, X_4, X_5)$ длины пять сократима.

Предположим противное. Заметим, что это означает, что никакая подпоследовательность нашей последовательности не сократима.

Посчитаем, сколько разных подпоследовательностей мы имеем.

- **Длина 0:** одна подпоследовательность (пустая).
- **Длина 1:** по крайней мере две разных подпоследовательности, так как в противном случае наша последовательность имела бы вид (X, X, X, X, X) и была бы сократима по теореме Гамильтона–Кэли.
- **Длина 2:** по крайней мере две подпоследовательности, так как совпадение (X_1, X_2) и (X_2, X_3) означает, что $X_1 = X_2 = X_3$, а последовательность (X, X, X) сократима по теореме Гамильтона–Кэли.
- **Длина 3:** по крайней мере две подпоследовательности по той же причине: совпадение (X_1, X_2, X_3) и (X_2, X_3, X_4) означает, что $X_1 = X_2 = X_3 = X_4$, а (X, X, X) сократима по теореме Гамильтона–Кэли.
- **Длина 4:** по крайней мере две подпоследовательности опять по той же причине: совпадение (X_1, X_2, X_3, X_4) и (X_2, X_3, X_4, X_5) означает, что $X_1 = X_2 = X_3 = X_4 = X_5$, а (X, X, X) сократима по теореме Гамильтона–Кэли.

Всего девять несократимых последовательностей мы насчитали. Заметим, что если у любого набора различных несократимых последовательностей взять произведения элементов, то полученные матрицы автоматически будут линейно независимыми (понятно, почему?). При этом размерность пространства матриц равна девяти, то есть через эти девять произведений не более чем четырёх сомножителей выражается всё (и наше произведение $X_1 X_2 X_3 X_4 X_5$, в частности).

Задача про матрицы 2×2 решается так же, но проще. Число 5 в этом случае можно заменить числом 3.

Решение 2. Пусть $M_n(\mathbb{C})$ обозначает пространство (алгебру) всех матриц размера $n \times n$ над полем комплексных чисел $\mathbb{C}$.

Рассмотрим некоторое произведение $U = B_1 \cdots B_l \in M_n(\mathbb{C})$. Обозначим через $\mathcal{S} = \{A_1, \dots, A_k\}$, $k \leqslant l$, — базис множества $B_1, \dots, B_l$. Далее будем считать $\mathcal{S}$ непустым, т.к. если $\mathcal{S}$ пусто, то $B_i = 0$ для всех i, и $U = 0 = B_1$.

Сделаем несколько очевидных наблюдений:

1. Достаточно решить задачу только для произведений, состоящих из l матриц из $\mathcal{S}$. (Разложим каждую матрицу B_r по базису $\mathcal{S}$, подставим в U и раскроем скобки.)

Пусть $\mathcal{L}_i(\mathcal{S})$ обозначает множество линейных комбинаций с коэффициентами из $\mathbb{C}$ (*линейную оболочку*) произведений не более i сомножителей элементов из $\mathcal{S}$. В частности, $\mathcal{L}_0(\mathcal{S}) = \{\alpha E | \alpha \in \mathbb{C}\}$, $\mathcal{L}_1(\mathcal{S}) = \{\alpha_0 E + \alpha_1 A_1 + \alpha_2 A_2 + \ldots + \alpha_k A_k | \alpha_0, \ldots, \alpha_k \in \mathbb{C}\}$ и т.п. Линейную оболочку всех возможных произведений матриц из $\mathcal{S}$ обозначим через $\mathcal{L}(\mathcal{S})$.

2. $\mathcal{L}(\mathcal{S})$ и $\mathcal{L}_i(\mathcal{S})$ являются подпространствами в $M_n(\mathbb{C})$, откуда, $\dim \mathcal{L}(\mathcal{S}), \dim \mathcal{L}_i(\mathcal{S}) \leqslant \dim M_n(\mathbb{C}) = n^2$.

3. Имеет место цепочка вложений $\mathcal{L}_0(\mathcal{S}) \subseteq \mathcal{L}_1(\mathcal{S}) \subseteq \ldots \subseteq \mathcal{L}_i(\mathcal{S}) \subseteq \ldots \subseteq \mathcal{L}_(\mathcal{S}) \subseteq M_n(\mathbb{C})$.

4. Если $\mathcal{L}_{i+1}(\mathcal{S}) = \mathcal{L}_i(\mathcal{S})$, то $\mathcal{L}_{i+j}(\mathcal{S}) = \mathcal{L}_i(\mathcal{S}) = \mathcal{L}(\mathcal{S})$ для любого $j \in \mathbb{N} \cup \{0\}$.

5. Если $\mathcal{L}_{i+1}(\mathcal{S}) \neq \mathcal{L}_i(\mathcal{S})$, то $\dim \mathcal{L}_{i+1}(\mathcal{S}) \geqslant \dim \mathcal{L}_i(\mathcal{S}) + 1$.

Случай $n = 2$:

Заметим, что $\dim M_2(\mathbb{C}) = 4$, поэтому возможны следующие варианты:

1. $\dim \mathcal{L}_1(\mathcal{S}) \leqslant 2$. Тогда $\mathcal{L}_1(\mathcal{S}) = \langle E, A \rangle$. По теореме Гамильтона–Кэли A^2 выражается в виде многочлена от E и A, откуда $\mathcal{L}_2(\mathcal{S}) = \mathcal{L}_1(\mathcal{S})$.

2. $\dim \mathcal{L}_1(\mathcal{S}) = 3$. Тогда либо $\mathcal{L}_2(\mathcal{S}) = \mathcal{L}_1(\mathcal{S})$, либо $\dim \mathcal{L}_2(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 1 = 4 = \dim M_2(\mathbb{C})$ и, следовательно, $\mathcal{L}_3(\mathcal{S}) = \mathcal{L}_2(\mathcal{S})$.

3. $\dim \mathcal{L}_1(\mathcal{S}) = 4 = \dim M_2(\mathbb{C})$. Тогда $\mathcal{L}_1(\mathcal{S}) = M_2(\mathbb{C})$ и, следовательно, $\mathcal{L}_k(\mathcal{S}) = \mathcal{L}_1(\mathcal{S})$ для любого $k \geqslant 2$.

Случай $n = 3$:

Во введенных обозначениях доказываемое утверждение примет вид: $W = A_{i_1} A_{i_2} A_{i_3} A_{i_4} A_{i_5} \in \mathcal{L}_4(\mathcal{S})$, здесь $A_i \in \mathcal{S}$ могут повторяться, и для решения задачи нам достаточно показать, что $\mathcal{L}(\mathcal{S}) = \mathcal{L}_4(\mathcal{S})$.

1. Если $\dim \mathcal{L}_1(\mathcal{S}) \leqslant 2$, то $W \in \mathcal{L}_2(\mathcal{S})$ как в случае $n = 2$.

2. Таким образом, далее мы будем считать, что $\dim \mathcal{L}(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) \geqslant 3$.

Если $\dim \mathcal{L}_1(\mathcal{S}) \geqslant \dim \mathcal{L}(\mathcal{S}) - 3$ и $\mathcal{L}_3(\mathcal{S}) \neq \mathcal{L}(\mathcal{S})$, то справедливо

$$\dim \mathcal{L}(\mathcal{S}) \geqslant \dim \mathcal{L}_4(\mathcal{S}) \geqslant \dim \mathcal{L}_3(\mathcal{S}) + 1 \geqslant \dim \mathcal{L}_2(\mathcal{S}) + 2 \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 3 \geqslant \dim \mathcal{L}(\mathcal{S}),$$

откуда, $\mathcal{L}(\mathcal{S}) = \mathcal{L}_4(\mathcal{S})$.

Мы показали, что если $\dim \mathcal{L}(\mathcal{S}) \leqslant 6$, то утверждение доказано.

3. Пусть теперь $7 \leqslant \dim \mathcal{L}(\mathcal{S}) \leqslant 9$ и $\dim \mathcal{L}(\mathcal{S}) - 4 \geqslant \dim \mathcal{L}_1(\mathcal{S}) \geqslant 3$.

Пусть $A_{i_1} A_{i_2} \in \mathcal{L}_1(\mathcal{S})$, или $A_{i_1} A_{i_2} A_{i_3} \in \mathcal{L}_2(\mathcal{S})$, или $A_{i_1} A_{i_2} A_{i_3} A_{i_4} \in \mathcal{L}_3(\mathcal{S})$, т.е. для некоторого $r \in \{2, 3, 4\}$ справедливо $A_{i_1} A_{i_2} \cdots A_{i_r} \in \mathcal{L}_{r-1}(\mathcal{S})$. По построению при этом также выполнено включение $A_{i_{r+1}} \cdots A_{i_5} \in \mathcal{L}_{5-r}(\mathcal{S})$. Поскольку степени многочленов при умножении складываются, из этих двух условий получаем, что

$$W = (A_{i_1} A_{i_2} \cdots A_{i_r}) \cdot (A_{i_{r+1}} \cdots A_{i_5}) \in \mathcal{L}_{(r-1)+(5-r)}(\mathcal{S}) = \mathcal{L}_4(\mathcal{S}).$$

Следовательно, можно считать, что $A_{i_1} A_{i_2} \cdots A_{i_r} \notin \mathcal{L}_{r-1}(\mathcal{S})$ ни для какого $r \in \{2, 3, 4\}$. Это означает, что $\dim \mathcal{L}_r(\mathcal{S}) \geqslant \dim \mathcal{L}_{r-1}(\mathcal{S}) + 1$ для всех $r \in \{2, 3, 4\}$, откуда как в пункте 2 получаем, что

$$\dim \mathcal{L}_4(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 3 \geqslant 6.$$

4. Допустим, что $\dim \mathcal{L}_2(\mathcal{S}) = \dim \mathcal{L}_1(\mathcal{S}) + 1$. В этом случае все одночлены степени 2 в $\mathcal{L}_2(\mathcal{S})$ представляются в виде линейной комбинации одночлена $A_{i_1} A_{i_2}$ и элементов из $\mathcal{L}_1(\mathcal{S})$. Тогда W есть линейная комбинация одночлена $A_{i_1}^3 A_{i_2} A_{i_5}$ и элементов из $\mathcal{L}_4(\mathcal{S})$. По теореме Гамильтона–Кэли для любой матрицы $A \in M_3(\mathbb{C})$ выполнено равенство $A^{3+l} = \alpha_{2_l} A^2 + \alpha_{1_l} A + \alpha_{0_l} E$, где $l \in \mathbb{N} \cup \{0\}$, $\alpha_i \in \mathbb{C}$. Поэтому, подставляя в W и раскрывая скобки, получим $W \in \mathcal{L}_4(\mathcal{S})$.

5. Пусть теперь $\dim \mathcal{L}_2(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 2$. В этом случае $\dim \mathcal{L}_4(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 4 \geqslant 7$.

Если $\dim \mathcal{L}(\mathcal{S}) = 7$, то $\dim \mathcal{L}_4(\mathcal{S}) = \dim \mathcal{L}(\mathcal{S})$, и все доказано.

При $\dim \mathcal{L}(\mathcal{S}) = 8$ и $\dim \mathcal{L}_1(\mathcal{S}) = 4$ получаем, что $\dim \mathcal{L}_4(\mathcal{S}) = 8 = \dim \mathcal{L}(\mathcal{S})$, $\mathcal{L}_4(\mathcal{S}) = \mathcal{L}(\mathcal{S})$, и все доказано.

При $\dim \mathcal{L}(\mathcal{S}) = 9$ и $\dim \mathcal{L}_1(\mathcal{S}) = 5$ также получаем, что $\dim \mathcal{L}_4(\mathcal{S}) = 9 = \dim \mathcal{L}(\mathcal{S})$, $\mathcal{L}_4(\mathcal{S}) = \mathcal{L}(\mathcal{S})$ и все доказано.

6. Значит, можно считать, что $\dim \mathcal{L}_1(\mathcal{S}) \leqslant 4$ при $\dim \mathcal{L}(\mathcal{S}) = 9$ и $\dim \mathcal{L}_1(\mathcal{S}) = 3$ при $\dim \mathcal{L}(\mathcal{S}) = 8$.

α. Предположим, что все одночлены степени 3 в $\mathcal{L}_3(\mathcal{S})$ представляются в виде линейных комбинаций $A_{i_1}A_{i_2}A_{i_3}$ и элементов из $\mathcal{L}_2(\mathcal{S})$. Тогда получим, что W представляется в виде линейной комбинации одночлена $A_{i_1}^3A_{i_2}A_{i_3} \in \mathcal{L}_4(\mathcal{S})$ (применение теоремы Гамильтона–Кэли аналогично п. 4) и элементов из $\mathcal{L}_4(\mathcal{S})$, т.е. $W \in \mathcal{L}_4(\mathcal{S})$.

β. Если предыдущий пункт не выполняется, то $\dim \mathcal{L}_3(\mathcal{S}) - \dim \mathcal{L}_2(\mathcal{S}) \geqslant 2$. В этом случае $\dim \mathcal{L}_4(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 5$.

- (a) В случае $\dim \mathcal{L}_1(\mathcal{S}) = 4$ получаем, что $\dim \mathcal{L}_4(\mathcal{S}) = 9 = \dim M_3(\mathbb{F})$, $\mathcal{L}_4(\mathcal{S}) = M_3(\mathbb{F})$, и все доказано.
- (b) Если $\dim \mathcal{L}_1(\mathcal{S}) = 3$ и $\dim \mathcal{L}(\mathcal{S}) = 8$, получаем, что $\dim \mathcal{L}_4(\mathcal{S}) = 8$, $\mathcal{L}_4(\mathcal{S}) = \mathcal{L}(\mathcal{S})$, и все доказано.
- (c) Осталось рассмотреть возможность $\dim \mathcal{L}_1(\mathcal{S}) = 3$ и $\mathcal{L}(\mathcal{S}) = M_3(\mathbb{C})$, внутри которой возможны два подслучая: либо $i_1 = i_2$, либо они различны.
  - (i) Если $i_1 = i_2$, то либо все произведения в $\mathcal{L}_4(\mathcal{S})$ представляются в виде линейной комбинации произведения $A_{i_1}^2A_{i_3}A_{i_4}$ и матриц из $\mathcal{L}_3(\mathcal{S})$, либо $\dim \mathcal{L}_4(\mathcal{S}) = 9$. Тогда в первом случае произведение W представляется в виде линейной комбинации произведения $A_{i_1}^3A_{i_3}A_{i_4}$ (лежит в $\mathcal{L}_4(\mathcal{S})$ по теореме Гамильтона–Кэли) и матриц из $\mathcal{L}_4(\mathcal{S})$, т.е. $W \in \mathcal{L}_4(\mathcal{S})$, а во втором случае все и так доказано.
  - (ii) Если $i_1 \neq i_2$, то либо $\dim \mathcal{L}_4(\mathcal{S}) = 9$ и $W \in \mathcal{L}_4(\mathcal{S}) = M_3(\mathbb{C})$, либо W представляется линейной комбинацией произведения $A_{i_1}^2A_{i_2}A_{i_3}A_{i_4}$ (лежит в $\mathcal{L}_4(\mathcal{S})$ по доказанному в i) и матриц из $\mathcal{L}_4(\mathcal{S})$. Следовательно, $W \in \mathcal{L}_4(\mathcal{S})$.

Упражнение 1. Приведите пример множества матриц $\mathcal{S}$, показывающий, что в 2×2-случае 3 нельзя заменить на меньшее число.

Упражнение 2. Приведите пример множества матриц $\mathcal{S}$, показывающий, что в 3×3-случае 5 нельзя заменить на меньшее число. Что в этом случае можно сказать про $\mathcal{L}(\mathcal{S})$?

Упражнение 3. Решите аналогичную задачу про матрицы 4×4.

Упражнение 4. Докажите, что найдутся две такие 3×3 матрицы, что любая 3×3 матрица может быть представлена в виде линейной комбинации произведений этих двух матриц. Верно ли соответствующее утверждение для $n > 3$?

Упражнение 5. На какое наименьшее число можно заменить пять в случае, когда все матрицы в произведении

а) диагональные,
б) верхненильтреугольные,
в) верхнетреугольные,
г) попарно коммутируют

в случае 3×3-матриц и в случае $n \times n$-матриц?