Семинар 7

Извлечение корня из перестановки

В этом тексте я хочу разобрать следующую задачу:

Задача. Найти все такие $\sigma \in S_8$, что $\sigma^2 = (1,2,3)(4,5,6)$.

Решение. В начале для удобства и единообразия добавим в запись правой части уравнения формальные циклы длины 1.

$$\sigma^2 = (1,2,3)(4,5,6)(7)(8)$$

Пусть σ какая-то перестановка, которая удовлетворяет этому уравнению. Она обязательно представляется в виде произведения независимых циклов: $\sigma = \rho_1 \dots \rho_k$. Так как циклы ρ_i независимы, то они коммутирую друг с другом, а значит:

$$\sigma^2 = \rho_1^2 \dots \rho_k^2 = (1,2,3)(4,5,6)(7)(8)$$

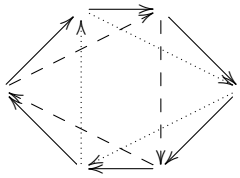
Что мы знаем про перестановки вида ρ_i^2. Если ρ_i – цикл нечетное длины, то ρ_i^2 остается циклом такой же длины, если ρ_i – цикл четной длины, то ρ_i^2 распадается в два цикла длины в два раза меньше. На основе этого соображения давайте поймем какие у нас есть варианты: либо $\rho_i^2 = (1,2,3)$, $\rho_i^2 = (4,5,6)$, $\rho_i^2 = (1,2,3)(4,5,6)$, $\rho_i^2 = (7)$, $\rho_i^2 = (8)$, $\rho_i^2 = (7)(8)$.

На самом деле, можно заметить, что достаточно извлечь корень из части $(1,2,3)(4,5,6)$ (при этом корень действует только на элементах $1,2,3,4,5,6$) и из части $(7)(8)$ (при этом корень действует только на элементах $7,8$), а потом перемножить между собой полученные варианты.

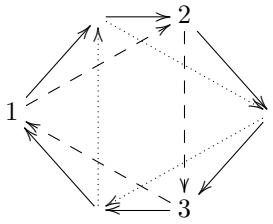
Давайте сначала извлечем корни из $(7)(8)$. У нас две возможности, либо цикл входящий в σ распадается при возведении в квадрат, либо не распадается. Если цикл не распадается, то он должен быть длины 1 ибо у нас оба цикла длины 1. То есть это значит $\sigma_2 = (7)(8)$. Если цикл не распадается, то он должен быть длины 2 ибо у нас два цикла длины один. То есть $\sigma_2 = (7,8)$. Это все возможные корни.

Теперь давайте извлечем корень из $(1,2,3)(4,5,6)$. Опять, у нас два цикла одинаковой длины. Потому цикл в σ либо распадается, либо не распадается. Давайте рассмотрим случай, когда цикл входящий в σ не распадается. Тогда $\rho_1^2 = (1,2,3)$ и одновременно $\rho_2^2 = (4,5,6)$. Здесь методом пристального взгляда (другой метод будет чуть ниже) видим, что корень извлекается единственным образом и равен $\rho_1 = (3,2,1)$ и $\rho_2 = (6,5,4)$. То есть у нас один вариант $\sigma_1 = (3,2,1)(6,5,4)$.

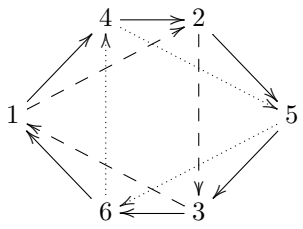
Теперь рассмотрим случай когда цикл из σ распадается. Тогда это должен быть цикл длины 6, который распадется в $(1,2,3)(4,5,6)$. То есть цикл должен выглядеть так

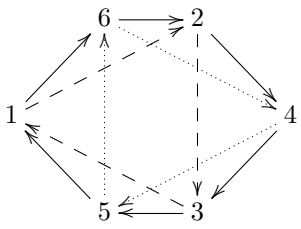


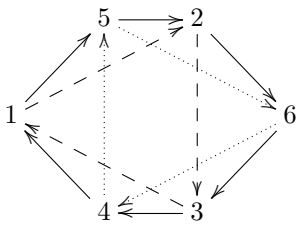
Где пунктиром отмечены циклы, в которые должен распасться наш цикл длины 6. Теперь вопрос, а как туда можно вписать наши циклы $(1,2,3)$ и $(4,5,6)$? Один цикл можно выбрать произвольно:



В второй цикл можно вписать тремя способами (три варианта для выбора стартовой вершины







То есть в распадающемся случае у нас 3 варианта для σ_1. То есть всего 4 варианта для σ_1.

А все решения имеют вид $\sigma = \sigma_1\sigma_2$. Всего получается 4 на 2 варианта, то есть 8.

Теперь давайте поясним вот какой момент, пусть мы хотим извлечь корень произвольной степени из цикла, то есть решить уравнение $\sigma^n = (1, \dots, m)$. Отметим, что если σ существует, то он тоже является циклом длины m. Действительно, разложим σ в независимые циклы. При возведении в степень количество циклов в σ^n может только увеличиться. А у нас получается один цикл. Значит и σ был одним циклом. С другой стороны, если цикл не распадается, то после возведения в степень он остается циклом той же длины.

Теперь давайте покажем, что если n и m взаимно просты, то корень извлекается однозначно. Так как n и m взаимно просты, то есть $1 = (n, m)$, то нод линейно выражается через m и n, то есть $1 = an + bm$. Возведем в степень a наше уравнение

$$(1, \dots, m)^a = \sigma^{an} = \sigma^{1-bm} = \sigma\left(\sigma^m\right)^{-b} = \sigma$$

Последнее равенство следует из того, что $\sigma^m = 1$ так как является циклом длины m. Так же отметим, что мы показали, что в случае $(m, n) = 1$ извлечение корня сводится к возведению в степень.

□

Еще немного о знаке

Один из основных вопросов – зачем нужен знак перестановки? Если кратко, то это очень хорошая характеристика, которая отличает некоторые ситуации. Чтобы быть предельно ясным, давайте разберем игру в пятнашки: у вас есть поле размером 3 на 5 и 14 фишек с номерами от 1 до 14 расставленных как на рисунке

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12 \\ 13 & 14 & \end{vmatrix}$$

Теперь враг переставляет эти фишки, пользуясь свободной ячейкой, и вам надо вернуть картинку в исходное состояние. И сразу возник вопрос, а что если рассмотреть расположение

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12 \\ 14 & 13 & \end{vmatrix}$$

Можно ли тогда вернуть фишки в исходное состояние? И оказывается ответ – нет. Но как доказывать подобные вещи? На самом деле надо рассмотреть инвариант похожий на знак перестановки и увидеть, что: (1) у этой позиции и начальной этот инвариант имеет разное значение, (2) при перестановке фишек, пользуясь свободной ячейкой, подобный инвариант не меняется.

Подробнее, рассмотрим произвольное расположение фишек на поле

$$\begin{vmatrix} 7 & 6 & 12 \\ 11 & 9 & 2 \\ 3 & & 5 \\ 14 & 10 & 13 \\ 8 & 1 & 4 \end{vmatrix}$$

По этому расположение построим перестановку нарезкой по строкам:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 7 & 6 & 12 & 11 & 9 & 2 & 3 & 5 & 14 & 10 & 13 & 8 & 1 & 4 \end{pmatrix}$$

После чего, берем знак этой перестановки. Заметим, что при перемещении фишек по горизонтали, перестановка σ не меняется, а при перемещении по вертикали, умножается на цикл длины 3. То есть четность не меняется при перемещении фишек.

Задача. Попробуйте модифицировать доказательство и покажите, что для поля размером 4 на 4 игра не выигрывается, если переставить местами фишки 14 и 15.

Определитель (напоминание)

Пусть $A \in \mathrm{M}_n(\mathbb{R})$ положим

$$\det A = \sum_{\sigma \in \mathrm{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)}$$

Это и есть определитель матрицы A. Думать про него надо так: пусть $A = (A_1 \mid \ldots \mid A_n)$ составлена из столбцов $A_i \in \mathbb{R}^n$. Тогда $\det A$ – это ориентированный объем n-мерного параллелепипеда натянутого на вектора $A_1, \ldots, A_n$.

Свойства определителя

1. Линейность по столбцу

   $$\det(A_1 \mid \ldots \mid A_i + A_i' \mid \ldots \mid A_n) = \det(A_1 \mid \ldots \mid A_i \mid \ldots \mid A_n) + \det(A_1 \mid \ldots \mid A_i' \mid \ldots \mid A_n)$$
   $$\det(A_1 \mid \ldots \mid \lambda A_i \mid \ldots \mid A_n) = \lambda \det(A_1 \mid \ldots \mid A_i \mid \ldots \mid A_n)$$

   Например,

   $$\det \begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix} = \det \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix} \middle| \begin{pmatrix} 3 \\ 7 \end{pmatrix} \right) = \det \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix} \middle| \begin{pmatrix} 1 \\ 3 \end{pmatrix} + \begin{pmatrix} 2 \\ 4 \end{pmatrix} \right) = \det \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} + \det \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$$

   Или для выноса коэффициента

   $$\det \begin{pmatrix} 1 & 3 \\ 2 & 9 \end{pmatrix} = 3 \det \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$$

2. Кососимметричность по столбцам

   $$\det(\ldots \mid A_i \mid \ldots \mid A_j \mid \ldots) = -\det(\ldots \mid A_j \mid \ldots \mid A_i \mid \ldots)$$

   Например,

   $$\det \begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix} = -\det \begin{pmatrix} 3 & 1 \\ 7 & 2 \end{pmatrix}$$

3. Кососимметричность по столбцам (другая форма)

   $$\det(\ldots \mid A \mid \ldots \mid A \mid \ldots) = 0$$

   Например,

   $$\det \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} = 0$$

4. $\det(A_1|\ldots|A_i|\ldots|A_j|\ldots|A_n) = \det(A_1|\ldots|A_i|\ldots|A_j + \lambda A_i|\ldots|A_n)$. То есть, если к одному столбцу матрицы прибавить другой умноженный на коэффициент, то определитель не изменится, например

   $$\det \begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix} = \det \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix} \middle| \begin{pmatrix} 3 \\ 7 \end{pmatrix} \right) = \det \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix} \middle| \begin{pmatrix} 3 \\ 7 \end{pmatrix} + 2 \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right) = \det \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix} \middle| \begin{pmatrix} 5 \\ 11 \end{pmatrix} \right) = \det \begin{pmatrix} 1 & 5 \\ 2 & 11 \end{pmatrix}$$

5. Единственность. Пусть $\phi\colon \mathrm{M}_n(\mathbb{R}) \to \mathbb{R}$ – функция на матрицах, которая кососимметрична и линейна по столбцам, тогда $\phi(X) = c \det(X)$, где константа $c = \phi(E)$ – значение в единичной матрице.

6. Согласованность с произведением. $\det(AB) = \det(A)\det(B)$. Получается применением предыдущего пункта к $\phi(X) = \det(AX)$.

7. Матрица A обратима тогда и только тогда, когда $\det A \neq 0$.

8. Согласованность с обращением. $\det(A^{-1}) = \det(A)^{-1}$, когда A обратима.

9. Согласованность с транспонированием. $\det(A) = \det(A^t)$. Следует из того, что $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$ и явной формулы определителя.

10. Линейность и кососимметричность по строкам. Следует из предыдущего пункта и соответствующих свойств по столбцам.

11. Определитель треугольной матрицы

$$\det\begin{pmatrix}\lambda_1 & * & \dots & * \\ & \lambda_2 & \dots & * \\ & & \ddots & \vdots \\ & & & \lambda_n\end{pmatrix} = \det\begin{pmatrix}\lambda_1 & & & \\ * & \lambda_2 & & \\ \vdots & \vdots & \ddots & \\ * & * & \dots & \lambda_n\end{pmatrix} = \lambda_1\lambda_2\dots\lambda_n$$

То есть у треугольной матрицы определитель равен произведению ее диагональных элементов. В частности $\det E = 1$ и $\det(\lambda E) = \lambda^n$.

12. Определитель блочной треугольной матрицы

$$\det\begin{pmatrix}A_1 & * & \dots & * \\ & A_2 & \dots & * \\ & & \ddots & \vdots \\ & & & A_k\end{pmatrix} = \det\begin{pmatrix}A_1 & & & \\ * & A_2 & & \\ \vdots & \vdots & \ddots & \\ * & * & \dots & A_k\end{pmatrix} = \det A_1 \dots \det A_k$$

где $A_i \in \mathrm{M}_{n_k}(\mathbb{R})$.

Определитель Вандермонда

Пусть нам даны числа $\lambda_1, \dots, \lambda_n \in \mathbb{R}$. Составим следующую матрицу размера n на n

$$W(\lambda_1, \dots, \lambda_n) = \begin{pmatrix}1 & 1 & \dots & 1 & 1 \\ \lambda_1 & \lambda_2 & \dots & \lambda_{n-1} & \lambda_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \lambda_1^{n-2} & \lambda_2^{n-2} & \dots & \lambda_{n-1}^{n-2} & \lambda_n^{n-2} \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \dots & \lambda_{n-1}^{n-1} & \lambda_n^{n-1}\end{pmatrix}$$

То есть в каждый столбец матрицы мы поставили степени каждого элемента λ_i с нулевой по $n-1$. Давайте покажем, что

$$\det(W(\lambda_1, \dots, \lambda_n)) = \prod_{j>i}(\lambda_j - \lambda_i)$$

Давайте я проделаю вычисления на примере $n = 4$. Тогда

$$\det(W) = \det\begin{pmatrix}1 & 1 & 1 & 1 \\ \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 \\ \lambda_1^2 & \lambda_2^2 & \lambda_3^2 & \lambda_4^2 \\ \lambda_1^3 & \lambda_2^3 & \lambda_3^3 & \lambda_4^3\end{pmatrix}$$

Давайте в начале вычтем предпоследнюю строку домноженную на λ_1 из последней, то есть третью из четвертой. Потом вычтем вторую с коэффициентом λ_1 из третьей. И в конце вычтем первую с коэффициентом λ_1 из второй. Это все преобразования третьего типа, потому у нас не поменяется определитель. Получим такую последовательность вычислений

$$\det\begin{pmatrix}1 & 1 & 1 & 1 \\ \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 \\ \lambda_1^2 & \lambda_2^2 & \lambda_3^2 & \lambda_4^2 \\ \lambda_1^3 & \lambda_2^3 & \lambda_3^3 & \lambda_4^3\end{pmatrix} = \det\begin{pmatrix}1 & 1 & 1 & 1 \\ \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 \\ \lambda_1^2 & \lambda_2^2 & \lambda_3^2 & \lambda_4^2 \\ 0 & \lambda_2^2(\lambda_2-\lambda_1) & \lambda_3^2(\lambda_2-\lambda_1) & \lambda_4^2(\lambda_2-\lambda_1)\end{pmatrix} =$$

$$= \det\begin{pmatrix}1 & 1 & 1 & 1 \\ \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 \\ 0 & \lambda_2(\lambda_2-\lambda_1) & \lambda_3(\lambda_2-\lambda_1) & \lambda_4(\lambda_2-\lambda_1) \\ 0 & \lambda_2^2(\lambda_2-\lambda_1) & \lambda_3^2(\lambda_2-\lambda_1) & \lambda_4^2(\lambda_2-\lambda_1)\end{pmatrix} = \det\begin{pmatrix}1 & 1 & 1 & 1 \\ 0 & \lambda_2-\lambda_1 & \lambda_3-\lambda_1 & \lambda_4-\lambda_1 \\ 0 & \lambda_2(\lambda_2-\lambda_1) & \lambda_3(\lambda_3-\lambda_1) & \lambda_4(\lambda_4-\lambda_1) \\ 0 & \lambda_2^2(\lambda_2-\lambda_1) & \lambda_3^2(\lambda_3-\lambda_1) & \lambda_4^2(\lambda_4-\lambda_1)\end{pmatrix}$$

Теперь заметим, что матрица разбивается на блоки и потому можно воспользоваться определителем с углом нулей

$$\det\left(\begin{array}{c|ccc}1 & 1 & 1 & 1 \\ \hline 0 & \lambda_2-\lambda_1 & \lambda_3-\lambda_1 & \lambda_4-\lambda_1 \\ 0 & \lambda_2(\lambda_2-\lambda_1) & \lambda_3(\lambda_3-\lambda_1) & \lambda_4(\lambda_4-\lambda_1) \\ 0 & \lambda_2^2(\lambda_2-\lambda_1) & \lambda_3^2(\lambda_3-\lambda_1) & \lambda_4^2(\lambda_4-\lambda_1)\end{array}\right) = 1 \cdot \det\begin{pmatrix}\lambda_2-\lambda_1 & \lambda_3-\lambda_1 & \lambda_4-\lambda_1 \\ \lambda_2(\lambda_2-\lambda_1) & \lambda_3(\lambda_3-\lambda_1) & \lambda_4(\lambda_4-\lambda_1) \\ \lambda_2^2(\lambda_2-\lambda_1) & \lambda_3^2(\lambda_3-\lambda_1) & \lambda_4^2(\lambda_4-\lambda_1)\end{pmatrix}$$

Но теперь можно из каждого столбца вынести общий множитель

$$\det\begin{pmatrix} \lambda_2-\lambda_1 & \lambda_3-\lambda_1 & \lambda_4-\lambda_1 \\ \lambda_2(\lambda_2-\lambda_1) & \lambda_3(\lambda_3-\lambda_1) & \lambda_4(\lambda_4-\lambda_1) \\ \lambda_2^2(\lambda_2-\lambda_1) & \lambda_3^2(\lambda_3-\lambda_1) & \lambda_4^2(\lambda_4-\lambda_1) \end{pmatrix} = (\lambda_2-\lambda_1)(\lambda_3-\lambda_1)(\lambda_4-\lambda_1)\det\begin{pmatrix} 1 & 1 & 1 \\ \lambda_2 & \lambda_3 & \lambda_4 \\ \lambda_2^2 & \lambda_3^2 & \lambda_4^2 \end{pmatrix}$$

И мы видим, что теперь нам надо посчитать определитель такого же вида, но только на размер меньше и не зависящий от λ_1, то есть $\det(W(\lambda_2,\lambda_3,\lambda_4))$. Теперь формально результат следует из индуктивного предположения.

Принцип «продолжения по непрерывности»

Задача. Рассмотрим квадратную матрицу из $\mathrm{M}_{n+m}(\mathbb{R})$ вида $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, где $A \in \mathrm{M}_n(\mathbb{R})$, $B \in \mathrm{M}_{n\,m}(\mathbb{R})$, $C \in \mathrm{M}_{m\,n}(\mathbb{R})$, $D \in \mathrm{M}_m(\mathbb{R})$. Покажите следующее:

1. Если A обратима, то
$$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(A)\det(D-CA^{-1}B)$$
2. Если $m=n$ и $AC=CA$, то[1]
$$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD-CB)$$

Решение. (1) Идея в том, чтобы применить блочные элементарные преобразования к строкам матрицы. А именно, мы берем первую строку матрицы $(A|B)$ и умножаем ее слева на «коэффициент» CA^{-1}, получим $(C|CA^{-1}B)$. После этого вычитаем эту строку из второй строки $(C|D)$ и получаем $(0|D-CA^{-1}B)$. На одной картинке мы проделали следующее

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \quad \text{вычитаем из II-ой строки I-ю умноженную на } CA^{-1} \text{ слева} \quad \longrightarrow \begin{pmatrix} A & B \\ 0 & D-CA^{-1}B \end{pmatrix}$$

По аналогии с элементарными преобразованиями первого типа над строками такая процедура не должна поменять определитель. Давайте строго поймем, почему определитель не меняется. Для этого заметим, что такая процедура эквивалентна умножению слева на блочную матрицу, а именно

$$\begin{pmatrix} E & 0 \\ -CA^{-1} & E \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ 0 & D-CA^{-1}B \end{pmatrix}$$

Самая левая матрица – нижнетреугольная с единицами на диагонали, а ее определитель равен 1. Потому определитель исходной матрицы равен определителю матрицы слева. А ее определитель равен требуемому, так как тут есть угол нулей.

(2) **Шаг 1** Давайте в начале рассмотрим случай A обратима. В этом случае, по первому пункту мы получаем

$$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det A\det(D-CA^{-1}B) = \det(AD-ACA^{-1}B) = \det(AD-CB)$$

В последнем равенстве мы воспользовались тем, что матрицы A и C коммутируют.

Шаг 2 А здесь я вам продемонстрирую идею, на которой держится решение многих задач. Например, если вы можете доказать что-то только для обратимых матриц, то этим способом очень легко свести доказательство необратимого случая к обратимому.

Давайте рассмотрим матрицу $A_\lambda = A - \lambda E$. Как мы знаем, спектр матрицы A – это в точности те λ, при которых $A-\lambda E$ необратима и таких λ у нас конечное число. А значит матрица A_λ необратима только для конечного числа λ и обратима для бесконечного числа λ.

Теперь рассмотрим нашу задачу для матрицы A_λ вместо матрицы A. То есть нам надо посчитать

$$\det\begin{pmatrix} A_\lambda & B \\ C & D \end{pmatrix}$$

[1] Обратите внимание, матрица A может не быть обратимой в этом случае.

Матрицы A и C коммутировали. Так как $A_\lambda = A - \lambda E$, то и A_λ и C коммутируют. А значит для всех $\lambda \in \mathbb{R}$ кроме конечного числа мы можем воспользоваться предыдущим шагом и написать

$$\det \begin{pmatrix} A_\lambda & B \\ C & D \end{pmatrix} = \det(A_\lambda D - CB) \quad \text{для всех } \lambda \in \mathbb{R} \text{ кроме конечного числа}$$

Теперь обратим внимание, что левая часть

$$\det \begin{pmatrix} A_\lambda & B \\ C & D \end{pmatrix}$$

является каким-то многочленом $f(\lambda)$. Действительно, если посчитать по формуле для определителя, то мы будем перемножать какие-то элементы из матриц $A - \lambda E$, B, C и D и потом складывать все вместе. Все элементы являются либо константами либо линейными многочленами от λ. А значит их произведение будет многочленом, ну и их сумма тоже. Аналогично правая часть

$$\det(A_\lambda D - CB)$$

тоже является каким-то многочленом $g(\lambda)$. И мы только что увидели, что $f(\lambda) = g(\lambda)$ для всех $\lambda \in \mathbb{R}$ кроме конечного числа. То есть многочлен $f - g$ имеет бесконечное число корней. А такое бывает лишь когда $f = g$, а значит $f(\lambda) = g(\lambda)$ вообще для любого числа $\lambda \in \mathbb{R}$. Подставим значение $\lambda = 0$ и получим желаемое. $\square$

На последний шаг можно смотреть так. Мы знаем результат для каждой матрицы A_λ в силу обратимости таких матриц при достаточно малом λ. А теперь в финальном равенстве переходим к пределу при $\lambda \to 0$. Это тоже корректное доказательство, но приведенное выше не использует анализ в явном виде. Кроме того, при правильных словах оно годится даже для экзотических полей вроде конечных (если вы понимаете о чем я говорю).