Продолжение алгебраических тождеств

Начнём с того, что не смогли довести до конца, а именно с вычисления определителя

$$\Delta = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \varepsilon & \varepsilon^2 & \dots & \varepsilon^{n-1} \\ 1 & \varepsilon^2 & \varepsilon^4 & \dots & \varepsilon^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \varepsilon^{n-1} & \varepsilon^{2(n-1)} & \dots & \varepsilon^{(n-1)^2} \end{pmatrix},$$

где ε — первообразный корень степени n из единицы. Прежде всего $\Delta = \prod_{n-1\geq i>j\geq 0}(\varepsilon^i - \varepsilon^j)$. Печаль состоит в том, что посчитать это выражение не легко, но можно посчитать его квадрат. А именно

$$\Delta^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(\varepsilon^i - \varepsilon^j) = (-1)^{\frac{n(n-1)}{2}} \prod_i \varphi'(\varepsilon^i) = n^n(-1)^{\frac{n(n-1)}{2}} \prod_i \varepsilon^{i(n-1)} = \pm n^n,$$

где $\varphi(x) = x^n - 1$. Теперь фиксируем конкретный первообразный корень $\varepsilon = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$. Мы хотим добиться положительности какого-то выражения от ε, чтобы установить, каким конкретно образом извлечь корень из Δ^2. Рассмотрим элемент $\varepsilon_1 = \cos(\frac{\pi}{n}) + i\sin(\frac{\pi}{n})$ — конкретный корень из ε. Тогда

$$\Delta = \prod_{n-1\geq i>j\geq 0}(\varepsilon^i - \varepsilon^j) = \prod_{i>j}(\varepsilon_1^{2i} - \varepsilon_1^{2j}) = \prod_{i>j}\varepsilon_1^{i+j}\prod_{i>j}(\varepsilon_1^{i-j} - \varepsilon_1^{j-i}) = \varepsilon_1^{\frac{n(n-1)^2}{2}} i^{\frac{n(n-1)}{2}} \prod_{i>j} 2\sin\tfrac{\pi(i-j)}{n}.$$

Последнее произведение положительно и следовательно равно $\sqrt{|\Delta^2|} = n^{\frac{n}{2}}$.

$$\Delta = n^{\frac{n}{2}}\varepsilon_1^{\frac{n(n-1)^2}{2}} i^{\frac{n(n-1)}{2}} = n^{\frac{n}{2}} i^{(n-1)^2+\frac{n(n-1)}{2}} = n^{\frac{n}{2}} i^{\frac{(n-1)(3n-1)}{2}}.$$

Вот такое вот вычисление. Из него, например, видно, что возможность извлечения корня из n завязана в поле зависит от наличия корней из единицы.

Теперь перейдём к новой теме, которую мы обсудили. Она называется принцип продолжения алгебраических тождеств. Тип задач, которые указанные методы позволяют решить следующий:
Пусть дано некоторое полиномиальное равенство вида $p(x_1,\dots,x_n) = 0$, которое можно доказать для достаточно большого числа значений $x_1,\dots,x_n$ из некоторого (коммутативного, как и везде) кольца K. Для каких ещё колец и каких $x_1,\dots,x_n$ справедливо это равенство?
Ответ на этот нечёткий вопрос такой же нечёткий: обычно равенство справедливо везде, где оно имеет смысл.

Особую тонкость составляет вопрос, когда равенство $p(x_1,\dots,x_n) = 0$ доказывалось при предположении о выполнимости некоторых тождеств для $x_1,\dots,x_n$. С каждой такой ситуацией приходится разбираться отдельно.

Техника доказательства таких тождеств лежит на трёх китах:

Кит 1. Пусть K — бесконечное или просто достаточно большое поле. Тогда, если многочлен $p(x_1,\dots,x_n) = 0$ для всех $x_1,\dots,x_n$, то он равен 0 в $K[x_1,\dots,x_n]$. На самом деле достаточно проверять для определённого конечного набора значений переменных.

Кит 2. Пусть R подкольцо в S. Тогда равенство $p(x_1,\dots,x_n) = 0$ для некоторых элементов $x_1,\dots,x_n \in R$ можно доказывать, как равенство для элементов из S. В частности, если R — область целостности, то в качестве S можно взять поле частных $Q(R)$ и применять все факты верные над полем. В частности, если $R = K[x_1,\dots,x_n]$ то при доказательстве тождества можно перейти к полю $K(t_1,\dots,t_n)$.

Кит 3. Если верно тождество $p(x_1,\dots,x_n) = 0$, как равенство внутри $R[x_1,\dots,x_n]$, то оно верно как тождество для любых элементов $x_1,\dots,x_n \in S$, где S — какая-то R-алгебра (при подходящей интерпретации коэффициентов p в S).

В частности, если верно $p(x_1,\dots,x_n) = 0$ для $p(x_1,\dots,x_n) \in \mathbb{Z}[x_1,\dots,x_n]$, то оно верно для любого кольца.

Приведём пример:

Предложение. *Пусть R — произвольное кольцо. Пусть A, B матрицы $n \times n$ над кольцом R. Тогда* $\det(AB) = \det(A)\det(B)$.

Доказательство. Заметим, что тождество $\det(AB) = \det(A)\det(B)$ полиномиально по элементам матриц a_{ij}, b_{ij} и у этого многочлена целые коэффициенты. То есть его можно проинтерпретировать как тождество в кольце $\mathbb{Z}[a_{11}, \ldots, a_{nn}, b_{11}, \ldots$ Для его доказательства перейдём к полю частных. Там оно очевидно верно(это поле). Тогда оно верно в $\mathbb{Z}[a_{11}, \ldots, a_{nn}, b_{11}, \ldots,$ тогда оно верно в любой $\mathbb{Z}$ алгебре, то есть в любом кольце.

Нам понадобится формула Крамера и её частный случай — формула для присоединённой матрицы.

Факт. Пусть дана система лин. уравнений $Ax = b$ с квадратной матрицей A над полем K. Если матрица A — обратима, то единственное решение этой системы имеет вид $x_i = \frac{\Delta_i}{\Delta}$, где $\Delta = \det A$, а Δ_i — определитель матрицы, полученной из A заменой i-го столбца на столбец b.

Определение 1. Присоединённой матрицей к матрице A называется матрица $\operatorname{Adj} A_{ij} = A_{ji}$ где A_{ij} — алгебраическое дополнение элемента a_{ij}.

Факт. Верен факт $\operatorname{Adj} A \cdot A = A \cdot \operatorname{Adj} A = \det(A) \cdot E$. В частности, есть формула (рациональная функция от коэффициентов A) для обратной матрицы.

Предложение. *Пусть R — произвольное кольцо. Пусть A матрица $n \times n$ над кольцом R. Тогда матрица A обратима тогда и только тогда , когда* $\det(A) \in R^*$ *— обратимый элемент.*

Доказательство. Заметим, что по предыдущему предложению $1 = \det(E) = \det(AA^{-1}) = \det(A)\det(A^{-1})$. Следовательно, если матрица обратима, то и определитель обратим. Обратно — рассмотрим тождества $\operatorname{Adj} A \cdot A = A \cdot \operatorname{Adj} A = \det(A) \cdot E$. Они верны в кольце $\mathbb{Z}[a_{11}, \ldots, a_{nn}]$, потому что верны в его поле частных. Следовательно верны в любом кольце. Остаётся только поделить на определитель A.

Следствие 1. *Матрица A из $M_n(\mathbb{Z})$ обратима тогда и только тогда, когда* $\det(A) = \pm 1$.

Теперь пусть у нас ситуация посложнее.

Предложение. *Пусть квадратные матрицы A и B над полем K коммутируют. Тогда*

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(DA - CB).$$

Доказательство. Здесь видны проблемы уже над полем. Для начала покажем, когда это тождество заведомо верно. Предположим, что матрица A обратима. Домножим матрицу

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \text{ слева на матрицу } \begin{pmatrix} E & 0 \\ -CA^{-1} & E \end{pmatrix}$$

Определитель от этого не изменится. Получится матрица

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

С другой стороны определитель этой матрицы равен

$$\det(A)\det(D - CA^{-1}B) = \det(DA - CA^{-1}BA) = \det(DA - CB).$$

Осталось понять, что тождество верно для действительно достаточно большого числа матриц A и B. Хотелось бы сказать, что мы доказали тождество в поле частных кольца $\mathbb{Z}[a_{ij}, b_{ij}, c_{ij}, d_{ij}]$. Однако это не так, ведь мы использовали тот факт, что $AB = BA$, то есть работали в кольце $\mathbb{Z}[a_{ij}, b_{ij}, c_{ij}, d_{ij}]/AB = BA$. Совершенно не очевидно, что это кольцо есть область целостности (на самом деле нам нужно меньше — только то, что элемент $\det A$ не делитель 0, тогда его можно формально обратить, но это тоже не очевидно).

Поступим по другому — введём дополнительный параметр λ и рассмотрим при фиксированных $A, B, C, D \in M_n(K)$ семейство

$$\begin{pmatrix} A - \lambda E & B \\ C & D - \lambda E \end{pmatrix}.$$

При любом λ в верхней строке стоят коммутирующие матрицы. Тогда заметим, что оба определителя есть многочлены от λ, которые совпадают почти везде (везде кроме корней уравнения $\det(A - \lambda E) = 0$). Этого может оказаться мало, если базовое поле K - конечно. Вместо K можно рассмотреть поле $K(\lambda)$, которое уже бесконечно (определитель — многочлен ненулевой степени, следовательно обратим, как элемент $K(\lambda)$). Тогда имеет место равенство многочленов от λ. Осталось подставить $\lambda = 0$. Для полей разобрались.

Задачи

Начнём с задачи про формулу Крамера.

Задача 1. Рассмотрим формальный ряд от переменной x с коэффициентами в кольце $\mathbb{R}$ заданный формулой

$$1 + b_1 x + b_2 x^2 + \cdots + b_n x^n + \cdots = \frac{x}{e^x - 1}.$$

Числами Бернулли называются выражения $B_n = (-1)^{n-1}(2n!)b_{2n}$. Покажите, что

$$B_n = (-1)^{n-1}(2n!)\begin{vmatrix} \frac{1}{2!} & 1 & 0 & \dots & 0 \\ \frac{1}{3!} & \frac{1}{2!} & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \frac{1}{2n!} & \dots & \frac{1}{3!} & \frac{1}{2!} & 1 \\ \frac{1}{(2n+1)!} & \frac{1}{2n!} & \dots & \frac{1}{3!} & \frac{1}{2!} \end{vmatrix}$$

Задача 2. Пусть R — произвольное кольцо, а A и B матрицы $n \times n$. Покажите, что $\det(E + AB) = \det(E + BA)$.

Задача 3. Доказать, что над произвольным кольцом R

$$\det\begin{pmatrix} b_1c_1 & b_1c_2 & \dots & b_1c_n \\ b_2c_1 & b_2c_2 & \dots & b_2c_n \\ \vdots & \vdots & \ddots & \vdots \\ b_nc_1 & b_nc_2 & \dots & b_nc_n \end{pmatrix} = 0$$

Задача 4. Пусть $n = 2k + 1$, а $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Найдите значение произведения

$$\prod_{0 \le l < k} (\varepsilon^k - \varepsilon^l).$$

Если вы вдруг не знаете

Задача 5. Посчитайте сумму

$$\sum_{l=0}^{n-1} \sin\frac{2\pi l}{n}.$$