Решения задач второй олимпиады

Задача 2007–1

Пусть P — квадратная матрица над полем рациональных чисел $\mathbb{Q}$. Докажите, что P обладает свойством $P^2 = P$ тогда и только тогда, когда $\operatorname{rk} P = \operatorname{tr} P$ и $\operatorname{rk}(E - P) = \operatorname{tr}(E - P)$. (*Предложил А. Э. Гутерман.*)

Решение 1. *Необходимость.* Пусть $P = P^2$. Тогда P задает оператор проектирования на подпространство $\operatorname{Im} P$ вдоль пространства $\operatorname{Ker} P$. Значит, $\operatorname{rk} P = \dim \operatorname{Im} P$ и ограничение $P|_{\operatorname{Im} P}$ — тождественный оператор на пространстве $\operatorname{Im} P$. Следовательно,

$$\operatorname{tr} P = \operatorname{tr}(P|_{\operatorname{Im} P}) = \dim \operatorname{Im} P = \operatorname{rk} P.$$

Также из $P = P^2$ следует, что $(E - P)^2 = E - P - P + P^2 = E - P$, и значит, по уже доказанному, выполняется и второе равенство.

Достаточность. Пусть $\operatorname{rk} P = \operatorname{tr} P$ и $\operatorname{rk}(E - P) = \operatorname{tr}(E - P)$. Тогда

$$\operatorname{rk}(E - P) = \operatorname{tr}(E - P) = n - \operatorname{tr} P = n - \operatorname{rk} P,$$

где n — размер матрицы. Следовательно,

$$\dim \operatorname{Ker} P + \dim \operatorname{Ker}(E - P) = n.$$

Очевидно, $\operatorname{Ker} P \cap \operatorname{Ker}(E - P) = \{0\}$, откуда

$$\mathbb{Q}^n = \operatorname{Ker} P \oplus \operatorname{Ker}(E - P).$$

Для любого вектора $x \in \operatorname{Ker}(E - P)$ справедливо $(E - P)x = 0$, то есть $x = Px$, откуда P действует тождественно на $\operatorname{Ker}(E - P)$. Следовательно, P — оператор проектирования вдоль $\operatorname{Ker} P$ на $\operatorname{Ker}(E - P) = \operatorname{Im} P$. Итак, $P = P^2$.

Решение 2. Приведем матричное доказательство, использующее только материал I семестра (в частности, не использующее операцию прямой суммы и соответствие между матрицами и операторами).

Лемма 1 («Начала алгебры»[1], теорема 9.16.13, стр. 223)**.** *Пусть $\mathbb{K}$ — произвольное поле, $A \in M_{m,n}(\mathbb{K})$, $\operatorname{rk} A = r > 0$. Тогда существуют такие $B \in M_{m,r}(\mathbb{K})$ и $C \in M_{r,n}(\mathbb{K})$, $\operatorname{rk} B = \operatorname{rk} C = r$, что $A = BC$.*

Доказательство. Пусть $\operatorname{rk} A = r$. Обозначим через $A_{i_1}, \ldots, A_{i_r}$ максимальную линейно независимую подсистему в системе строк $A_1, \ldots, A_m$ матрицы A. Тогда существуют такие $\beta_{ij} \in \mathbb{K}$, что

$$A_i = \beta_{i1} A_{i_1} + \ldots + \beta_{ir} A_{i_r}, \quad 1 \leqslant i \leqslant m.$$

Рассмотрим матрицу $B \in M_{m,r}(\mathbb{K})$, $B = (\beta_{ij})$, и матрицу $C \in M_{r,n}(\mathbb{K})$, у которой j-тая строка C_j равна A_{i_j}, $j = 1, \ldots, r$. Тогда $A = BC$. Условие $\operatorname{rk} B = \operatorname{rk} C = r$ выполняется в силу неравенства $\operatorname{rk}(BC) \leqslant \min\{\operatorname{rk} B, \operatorname{rk} C\}$. □

Лемма 2. *Пусть $\mathbb{K}$ — произвольное поле, $P \in M_n(\mathbb{K})$, $\operatorname{rk} P = r$. Докажем, что $P^2 = P$ тогда и только тогда, когда существуют $B \in M_{n,r}(\mathbb{K})$, $C \in M_{r,n}(\mathbb{K})$, $\operatorname{rk} B = \operatorname{rk} C = r$, такие, что $P = BC$ и $CB = E_r$ — единичная $r \times r$-матрица.*

Доказательство. Достаточность: $P^2 = BCBC = BE_rC = BC = P$.

Необходимость: $\operatorname{rk} P = r$. Следовательно, по лемме 1, существуют такие $B \in M_{n,r}(\mathbb{K})$ и $C \in M_{r,n}(\mathbb{K})$, $\operatorname{rk} B = \operatorname{rk} C = r$, что $P = BC$. Так как B и C — матрицы полного ранга, существуют матрицы $(B^\top B)^{-1}$ и $(CC^\top)^{-1}$. По условию $P^2 = P$, то есть $BCBC = BC$. Умножим последнее равенство слева на $(B^\top B)^{-1}B^\top$ и справа на $C^\top(CC^\top)^{-1}$. Имеем:

$$(B^\top B)^{-1}B^\top \cdot BCBC \cdot C^\top(CC^\top)^{-1} = (B^\top B)^{-1}B^\top \cdot BC \cdot C^\top(CC^\top)^{-1},$$

откуда, $CB = E_r \cdot E_r = E_r$. Тем самым лемма доказана. □

[1] А. В. Михалев, А. А. Михалев, *Начала алгебры. Часть 1.* Москва: Интернет-университет информационных технологий, 2005.

Обозначим $\operatorname{rk} P = r$. Пусть $E \in M_n(\mathbb{K})$ — единичная матрица. Если $r = 0$, то утверждение теоремы тривиально. Далее будем считать $r > 0$.

Необходимость. 1. Докажем, что если $P = P^2$, то $\operatorname{rk} P = \operatorname{tr} P$. Представим P в виде $P = BC$, где $CB = E_r$ по лемме 2. Тогда

$$\operatorname{tr} P = \operatorname{tr}(BC) = \operatorname{tr}(CB) = \operatorname{tr} E_r = r = \operatorname{rk} P.$$

2. Докажем, что если $P = P^2$, то $(E - P)^2 = E - P$.

Так как $P^2 = P$, имеем:

$$(E - P)^2 = E - P - P + P^2 = E - P.$$

3. Докажем, что если $P = P^2$, то $\operatorname{rk} P = \operatorname{tr} P$ и $\operatorname{rk}(E - P) = \operatorname{tr}(E - P)$.

По пункту 2, $(E - P)^2 = E - P$. остальное следует из пункта 1.

Достаточность: докажем, что если $\operatorname{rk} P = \operatorname{tr} P$ и $\operatorname{rk}(E - P) = \operatorname{tr}(E - P)$, то $P = P^2$.

По условию имеем

$$\operatorname{rk}(E - P) = \operatorname{tr}(E - P) = n - \operatorname{tr} P = n - \operatorname{rk} P.$$

Используя лемму 1, запишем $P = BC$ и $E - P = DG$, где $B \in M_{n,r}(\mathbb{K})$, $C \in M_{r,n}(\mathbb{K})$, $\operatorname{rk} B = \operatorname{rk} C = r$ и $D \in M_{n,s}(\mathbb{K})$, $G \in M_{s,n}(\mathbb{K})$, $\operatorname{rk} D = \operatorname{rk} G = s = n - r$. Тогда

$$E = P + (E - P) = BC + DG = RS,$$

где $R = (B|D) \in M_n(\mathbb{K})$, $S = \begin{pmatrix} C \\ G \end{pmatrix} \in M_n(\mathbb{K})$ — объединения матриц B и D, C и G, соответственно, то есть, R и S — взаимно обратные матрицы:

$$\begin{pmatrix} C \\ G \end{pmatrix} (B|D) = \begin{pmatrix} E_r & 0 \\ 0 & E_s \end{pmatrix}.$$

Следовательно, $CB = E_r$, откуда $P^2 = P$ по лемме 1.

Решение 3. Приведем доказательство с использованием жордановой нормальной формы.

По теореме о жордановой нормальной форме, существует матрица $S \in \mathbf{GL}_n(\mathbb{C})$, такая, что $J_P = SPS^{-1}$, где $J_P \in M_n(\mathbb{C})$ — жорданова нормальная форма матрицы $P \in M_n(\mathbb{Q}) \subseteq M_n(\mathbb{C})$.

Необходимость. $P = P^2$, следовательно, $q(x) = x(x - 1)$ — аннулирующий многочлен матрицы P. Тогда ее собственные числа принадлежат множеству $\{0, 1\}$ и все жордановы клетки имеют размер 1, то есть, J_P — диагональная матрица с 0 и 1 на главной диагонали. Следовательно,

$$\operatorname{rk} J_P = \operatorname{tr} J_P \text{ и } \operatorname{rk}(E - J_P) = \operatorname{tr}(E - J_P),$$

откуда

$$\operatorname{rk} P = \operatorname{tr} P \text{ и } \operatorname{rk}(E - P) = \operatorname{tr}(E - P).$$

Достаточность. Пусть матрица J_P содержит $k_0 \geqslant 0$ жордановых клеток, соответствующих собственному значению 0, и $k_1 \geqslant 0$ жордановых клеток, соответствующих собственному значению 1. Тогда

$$\operatorname{rk} P = \operatorname{rk} J_P = n - k_0, \quad \operatorname{rk}(E - P) = \operatorname{rk}(E - J_P) = n - k_1.$$

По условию отсюда следует, что $\operatorname{tr} P = n - k_0$, $\operatorname{tr}(E - P) = n - k_1$. С другой стороны, $\operatorname{tr} P + \operatorname{tr}(E - P) = \operatorname{tr} E = n$. Следовательно, $k_0 + k_1 = n$. Итак, получаем, что все жордановы клетки имеют размер 1 и других собственных чисел кроме 0 и 1 у матрицы P нет. Тогда, с точностью до перестановки строк и столбцов,

$$J_P = \operatorname{diag}\{\underbrace{1, \ldots, 1}_{k_1}, \underbrace{0, \ldots, 0}_{k_0}\}.$$

Значит, $J_P^2 = J_P$, откуда $P^2 = P$.

Упражнение 1. При каких условиях на основное поле утверждение остается справедливым?

Упражнение 2. Как мы выяснили, след и ранг проектора совпадают. Приведите примеры других линейных операторов, у которых эти инварианты совпадают.

Задача 2007–2

Студент Д. решил возвести все матрицы 17×17 над полем из семнадцати элементов в сотую степень, сложить результаты и посмотреть, что получится. Но в этот момент у студента сломался компьютер. Помогите ему. (*Предложил А. А. Клячко.*)

Решение 1. Просуммируем отдельно пропорциональные между собой матрицы:

$$\sum_{A\in M_{17}(\mathbb{Z}_{17})} A^{100} = 0^{100} + \sum_{i=1}^{l} \left(A_i^{100} + (2A_i)^{100} + (3A_i)^{100} + \dots + (16A_i)^{100}\right) =$$

$$= \left(1^{100} + 2^{100} + \dots + 16^{100}\right) \sum_{i=1}^{l} A_i^{100},$$

где l есть число непропорциональных друг другу ненулевых матриц (то есть $l = \frac{17^{17^2}-1}{17-1}$). Вспоминая, что мультипликативная группа конечного поля является циклической, мы получаем, что в $\mathbb{Z}_{17}$

$$1^{100} + 2^{100} + \dots + 16^{100} = 1 + a^{100} + a^{200} + a^{300} + \dots + a^{1500},$$

где a — порождающий элемент группы $\mathbb{Z}_{17}^*$ (в качестве a можно взять, например, тройку). Суммируя получившуюся геометрическую прогрессию, мы видим, что

$$1 + a^{100} + a^{200} + a^{300} + \dots + a^{1500} = \frac{a^{1600}-1}{a^{100}-1} = \frac{0}{\text{не ноль}} = 0.$$

Таким образом, интересующая студента Д. сумма равна нулевой матрице.

Решение 2. Умножим каждую матрицу $A \in M_{17}(\mathbb{Z}_{17})$ на порождающий элемент a группы $\mathbb{Z}_{17}^*$. С одной стороны, сумма сотых степеней всех матриц от этого не изменится (просто, слагаемые переставятся), а с другой стороны, эта сумма умножится на $a^{100} \neq 1$. Отсюда следует, что интересующая студента Д. матрица нулевая.

Упражнение. Что будет, если число 100 в этой задаче заменить на 80?

Задача 2007–3

Проверив сто контрольных по алгебре, доцент Л. И. Нейный обнаружил, что из полученных оценок нельзя составить невырожденную матрицу. Доцент очень расстроился, исправил одну из единиц на двойку, составил из оценок матрицу с определителем сто шестьдесят два, успокоился и лег спать. Какие оценки получили студенты? (Теоретически, оценки бывают такие: 1, 2, 3, 4 и 5.) (*Предложил А. А. Клячко.*)

Решение. Докажем сперва лемму.

Лемма 1. *Из набора положительных чисел $a_1, \dots, a_{n^2}$ нельзя составить невырожденную матрицу тогда и только тогда, когда одно из чисел встречается в этом наборе более $n^2 - n + 1$ раз.*

Доказательство. Если число a встречается в матрице $n \times n$ более $n^2 - n + 1$ раз, то все элементы по крайней мере двух строк этой матрицы равны a и, следовательно, матрица вырождена, поскольку имеет две одинаковые строки.

Докажем в другую сторону. Пусть никакое число не встречается в наборе более $n^2 - n + 1$ раз. Расставим элементы матрицы A так, чтобы каждая строка, кроме, возможно, первой, содержала по крайней мере два разных элемента.

Используя индукцию по n, мы можем считать, что минор $M_{n,n}$ матрицы A отличен от нуля и, следовательно первые $n-1$ строк нашей матрицы линейно независимы. Если вся матрица при этом является вырожденной, то последняя строка выражается через остальные строки. Воспользуемся следующим известным простым фактом:

> *всевозможные перестановки строки $(x_1, \dots, x_n)$ порождают все арифметическое векторное пространство F^n, если $\sum x_i \neq 0$ и не все x_i равны между собой.*[2] (Докажите!)

Отсюда следует, что некоторая перестановка последней строки нашей матрицы не лежит в линейной оболочке первых $n-1$ строк и, следовательно, соответствующая матрица является невырожденной. Лемма доказана. □

[2]Другими словами, можно сказать так: *естественное n-мерное представление симметрической группы $\mathbf{S}_n$ содержит ровно два ненулевых собственных подпредставления.*

Из этой леммы и из условий задачи вытекает, что изначально доцент Л. И. Нейный поставил ровно 92 единицы, и мы приходим к такой ситуации: матрица A размера 10×10 состоит из 91 единицы, оставшиеся 9 элементов $z_1,\dots,z_9$ принадлежат множеству $\{2,3,4,5\}$ и $\det A = 162$. Из невырожденности этой матрицы следует, что в каждой строке, кроме одной, и в каждом столбце, кроме одного, имеется ровно один неединичный элемент. Переставим строки и столбцы так, чтобы неединичные элементы оказались на главной диагонали, а строка из единиц оказалась последней (при этом может измениться лишь знак определителя). Вычитая из всех строк последнюю, мы приходим к треугольной матрице, на диагонали которой стоят числа $z_1-1,\dots,z_9-1,1$. Таким образом, $162 = 3^4\cdot 2 = \det A = \pm(z_1-1)\dots(z_9-1)$, то есть среди z_i имеются четыре четверки, одна тройка и четыре двойки. Остальные оценки — единицы.

Упражнение. Из каких наборов n^2 комплексных чисел можно составить невырожденную матрицу? Найдите необходимые и достаточные условия. (Ответ не совсем очевиден.)

Задача 2007–4

Пусть $\mathbb{K}$ — произвольное поле. Покажите, что всякая подалгебра алгебры $\mathbb{K}[x]$ конечно порождена, то есть является гомоморфным образом алгебры многочленов от конечного числа переменных. Верно ли аналогичное утверждение для произвольной подалгебры в $\mathbb{K}[x,y]$? (*Предложил И. В. Аржанцев.*)

Решение. *Этап 1.* Пусть P — такое непустое подмножество во множестве целых неотрицательных чисел $\mathbb{N}_0$, что $a+b\in P$ для любых $a,b\in P$. Докажем, что найдутся такие числа $a_1,\dots,a_m\in P$, что любой элемент из P можно получить складывая (возможно, многократно) эти числа. Другими словами, докажем, что всякая подполугруппа в $\mathbb{N}_0$ конечно порождена.

Пусть D — множество натуральных чисел, которые делят все числа из множества P. Ясно, что $1\in D$ и для каждого $a\in P$ все элементы D не превосходят a. Пусть d — наибольший элемент в D. Тогда найдется конечный набор чисел $b_1,\dots,b_n$ из P, наибольший общий делитель которых равен d. Значит, существуют целые $u_1,\dots,u_n$, для которых $u_1b_1+\dots+u_nb_n=d$. Прибавляя к этому равенству равенства $(-b_i)b_1+b_1b_i=0$, мы получим выражение $u_{11}b_1+\dots+u_{1n}b_n=d$, где $u_{11}<0$, $u_{12}>0,\dots,u_{1n}>0$. Аналогично можно получить равенства $u_{i1}b_1+\dots+u_{in}b_n=d$, в которых единственным отрицательным коэффициентом является u_{ii}. Пусть U — это наибольшее из чисел $-u_{11},\dots,-u_{nn}$. Тогда $Ub_1+\dots+Ub_n=md$ для некоторого натурального m. Далее, $(U+u_{11})b_1+\dots+(U+u_{1n})b_n=(m+1)d$. В этом выражении один из коэффициентов (скажем, j-й) больше U. Прибавляя к нему $u_{j1}b_1+\dots+u_{jn}b_n=d$, получаем выражение для $(m+2)d$, и т.д. Тем самым доказано, что все числа большие md и делящиеся на d можно получить, складывая $b_1,\dots,b_n$. Остается в качестве чисел $a_1,\dots,a_m$ взять все элементы множества P, меньшие md. (Числа $b_1,\dots,b_n$ туда тоже войдут.)

Этап 2. Пусть A — некоторая подалгебра в $\mathbb{K}[x]$, $P:=\{\deg f\mid f\in A\}$ и $a_1,\dots,a_m$ — набор чисел в P, построенный на предыдущем шаге. Зафиксируем элементы $f_i\in A$, $\deg(f_i)=a_i$, и покажем, что образом гомоморфизма

$$\mathbb{K}[T_1,\dots,T_m]\to\mathbb{K}[x],\qquad T_i\mapsto f_i$$

является подалгебра A. Для этого достаточно показать, что каждый элемент из A выражается через многочлены 1, f_1, …, f_m. Будем доказывать это индукцией по степени. Для многочленов степени ноль утверждение очевидно. Далее, для любого $F\in A$ его степень $\deg F$ равна $k_1a_1+\dots+k_ma_m$ для некоторых целых неотрицательных $k_1,\dots,k_m$. Значит, если вычесть из F многочлен $f_1^{k_1}\dots f_m^{k_m}$ с подходящим коэффициентом, получится многочлен меньшей степени, и к нему можно применить предположение индукции.

Этап 3. Наконец, рассмотрим подалгебру A в $\mathbb{K}[x,y]$, состоящую из многочленов, в которых каждый член, отличный от свободного члена, делится на x. Предположим, что она порождена многочленами

$$f_1(x,y),\ \dots,\ f_m(x,y).$$

Пусть M есть максимум отношений $\frac{j}{i}$ по всем одночленам αx^iy^j, где $i+j>0$, $0\neq\alpha\in\mathbb{K}$, входящим в $f_1,\dots,f_m$. Тогда многочлен xy^{M+1} лежит в A и не выражается через $f_1,\dots,f_m$. Противоречие.

Упражнение. Пусть $\mathbb{K}$ — произвольное поле и A — конечно порожденная коммутативная ассоциативная алгебра над $\mathbb{K}$ с единицей и без делителей нуля. Докажите, что любая подалгебра в A конечно порождена тогда и только тогда, когда любые два элемента из A алгебраически зависимы.

Задача 2007–5

Пусть w — бесконечное слово в двоичном алфавите $\{0,1\}$. *Сложностью* такого слова называется функция $c_w : \mathbb{N} \to \mathbb{N}$, определяемая как $c_w(n) =$ *число различных подслов в* w *длины* n. (Подслово — это набор символов, идущих в слове w подряд.)

(1) Докажите, что слово w с некоторого момента становится периодическим тогда и только тогда, когда $c_w(n) \leqslant n$ для некоторого $n \geqslant 1$.

(2) Постройте слово, для которого $c_w(n) = n+1$ для всех $n = 1, 2, \ldots$, и которое ни с какого момента периодическим не становится.

(*Предложил М. В. Зайцев*[3].)

Решение.

Часть 1. Пусть слово w становится периодическим начиная с k-й позиции и длина этого периода равна m. Тогда очевидно, что $c_w(k+m) \leqslant k+m$.

Наоборот, пусть $c_w(n) \leqslant n$. Если слово состоит только из нулей или только из единиц, то оно, конечно, периодическое. В противном случае $c_w(1) = 2$. Заметим, что функция c_w неубывающая. Докажем сначала, что для некоторого $s \geqslant 1$ выполняется $c_w(s) = c_w(s+1)$. Действительно, если $c_w(k-1) < c_w(k)$ для всех $k = \overline{1,n}$, то получаем противоречие:

$$c_w(n) \geqslant c_w(n-1) + 1 \geqslant \ldots \geqslant c_w(1) + n - 1 = n + 1.$$

Итак, пусть $r = c_w(s) = c_w(s+1)$. Пусть $u_1, \ldots, u_r$ — все подслова в w длины s. Тогда каждое слово длины $s+1$ получается из одного и только одного слова этого набора приписыванием символа 0 или 1. Другими словами, после каждого слова u_i может идти только один соответствующий этому слову символ. Пусть v_k — подслово в w длины s, начинающееся с позиции k. Ясно, что $v_k \in \{u_1, \ldots, u_r\}$ и v_{k+1} однозначно определяется по значению v_k. Тогда $\{v_k\}$ начиная с некоторого момента становится периодической последовательностью. Значит, само слово w с некоторого момента становится периодическим.

Часть 2. Заметим, что в силу первой части задачи достаточно построить слово w, для которого $c_w(n) = n+1$ для всех $n \in \mathbb{N}$. Такие слова называются *словами Штурма*.

Будем называть подслово u слова w *специальным*, если w обладает подсловами $u0$ и $u1$.

Упражнение 1. Слово w является словом Штурма тогда и только тогда, когда для каждого $n \geqslant 0$ оно обладает ровно одним специальным подсловом длины n.

Мы построим так называемое *слово Фибоначчи*, являющееся словом Штурма.

Определим функцию φ из алфавита $\{0,1\}$ в множество всех слов:

$$\varphi(x) = \begin{cases} 01, & x = 0; \\ 0, & x = 1. \end{cases}$$

Распространим эту функцию посимвольно на все слова. Рассмотрим последовательность слов $f_n = \varphi^n(0)$, $n \geqslant 0$. Заметим, что

$$f_0 = 0, \quad f_1 = 01, \quad f_{n+2} = f_{n+1} f_n,$$

то есть, каждое слово является префиксом всех следующих. Будем также для удобства считать, что $f_{-1} = 1$. Пусть f — бесконечное слово, получающееся из $f_0, f_1, \ldots$ «в пределе» (можно сказать, что k-й символ слова f есть k-й символ слова f_k). Длины слов f_k образуют последовательность чисел Фибоначчи, откуда и происходит название слова f. Первые символы этого слова таковы:

$$f = 0100101001001010010100100101001001\ldots.$$

Так как $f = \varphi(f)$, то f раскладывается на подслова вида 01 и 0. Поэтому 11 не является подсловом в f и $c_f(2) = 3$. Слово 000 также не является подсловом в $\varphi(f)$, так как в противном случае оно было бы префиксом некоторого слова $\varphi(x)$ для подслова x в f и это подслово x начиналось бы с 11.

Докажем, что f обладает ровно одно одним специальным подсловом каждой длины.

Этап 1. Покажем, что ни для какого слова x слова $0x0$ и $1x1$ не могут одновременно являться подсловами в f. Это очевидно, если длина x равна 0 или 1. Воспользуемся индукцией по длине. Предположим $0x0$ и $1x1$ — подслова в f. Тогда x должно начинаться и заканчиваться нулем: $x = 0y0$ для некоторого слова y. Так как $00y00$ и $10y01$ должны быть подсловами в $\varphi(x)$, должно существовать

[3] Подробнее про эту задачу см. книгу Lothaire, M. (2002). Algebraic Combinatorics on Words. Cambridge UK: Cambridge University Press.

подслово z в f, такое, что $\varphi(z) = 0y$. Более того, $00y0 = \varphi(1z1)$ и $010y01 = \varphi(0z0)$. Мы получаем противоречие с тем, что для слова z меньшей длины подслова $1z1$ и $0z0$ входят в f.

Этап 2. Покажем, что у f есть не более одного специального подслова каждой длины. Предположим противное: пусть u и v — разные специальные подслова в f равной длины. Пусть x — наибольший общий суффикс этих подслов. Тогда $0x0$, $0x1$, $1x0$ и $1x1$ — подслова в f, что невозможно.

Упражнение 2. Пусть $\widetilde{u}$ обозначает слово, записанное символами из u в обратном порядке. Докажите, что $\varphi(\widetilde{u})\,0 = 0\,\widetilde{\varphi(u)}$.

Этап 3. Мы построим специальные подслова в f вида $\widetilde{f_n}$. Докажем по индукции, что при $n \geqslant 2$ слово f_{n+2} можно представить в виде

$$f_{n+2} = g_n\,\widetilde{f_n}\,\widetilde{f_n}\,t_n,$$

где $g_2 = \varepsilon$ — пустое слово, $g_n = f_{n-3}\dots f_1 f_0$ при $n \geqslant 2$ и

$$t_n = \begin{cases} 01, & \text{если } n \text{ нечетное,} \\ 10, & \text{если } n \text{ четное.} \end{cases}$$

В самом деле, $f_4 = \varepsilon(010)(010)10$ и $f_5 = 0(10010)(10010)01$. Далее, из упражнения следует, что

$$\varphi(\widetilde{f_n}\,t_n) = \varphi(\widetilde{f_n})\,\varphi(t_n) = \varphi(\widetilde{f_n})\,0\,t_{n+1} = 0\,\widetilde{f_{n+1}}\,t_{n+1}.$$

Так как $\varphi(g_n)0 = g_{n+1}$, мы получаем

$$f_{n+3} = \varphi(f_{n+2}) = \varphi(g_n)\,\varphi(\widetilde{f_n})\,\varphi(\widetilde{f_n}\,t_n) = \varphi(g_n)\,\varphi(\widetilde{f_n})\,0\,\widetilde{f_{n+1}}\,t_{n+1} =$$
$$\varphi(g_n)\,0\,\widetilde{\varphi(f_n)}\,\widetilde{f_{n+1}}\,t_{n+1} = g_{n+1}\,\widetilde{f_{n+1}}\,\widetilde{f_{n+1}}\,t_{n+1}.$$

Заметим, что первый символ в $\widetilde{f_n}$ отличен от первого символа в t_n. Поэтому $\widetilde{f_n}$ — специальное подслово в f. Всякий суффикс специального подслова является специальным, поэтому в f существуют специальные подслова любой длины.

Задача 2007–6

Назовем коммутативное ассоциативное кольцо с единицей *дюжинным*, если каждое отображение из этого кольца в себя задается многочленом 12-й степени над этим кольцом. Опишите все дюжинные кольца. (*Предложил А. А. Клячко.*)

Решение. Отметим сразу, что нулевое кольцо можно назвать кольцом с единицей, но нельзя назвать дюжинным по формальным причинам. (Понимаете, почему?)

Пусть R — дюжинное кольцо. В частности, отображение

$$\delta(a) = \begin{cases} 1, & \text{если } a \neq 0, \\ 0, & \text{если } a = 0 \end{cases}$$

задается некоторым многочленом $f(x) = \sum\limits_{i=0}^{12} c_i x^i$, где $c_i \in R$. Тогда $f(0) = c_0 = 0$ и для каждого $b \neq 0$

$$f(b) = b\sum_{i=1}^{12} c_i b^{i-1} = 1,$$

откуда вытекает, что всякий ненулевой элемент $b \in R$ обратим, то есть R — поле.

Поле, содержащее больше двенадцати элементов, не может быть дюжинным, поскольку в дюжинном кольце нулевая функция задается многочленом двенадцатой степени, а число корней ненулевого многочлена над полем не превосходит его степени.

С другой стороны, каждое поле $F = \{a_1, \dots, a_q\}$, содержащее не больше двенадцати элементов, является дюжинным. Действительно, согласно интерполяционной теореме Лагранжа каждое отображение $\varphi : F \to F$ задается многочленом $f(x)$, степень которого не превосходит $q-1$, а многочлен двенадцатой степени

$$g(x) = f(x) + x^{12-q}(x - a_1)(x - a_2)\dots(x - a_q)$$

задает то же самое отображение φ.

Таким образом, дюжинные кольца — это то же самое, что поля, содержащие не больше двенадцати элементов, то есть $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$, $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_8$, $\mathbb{F}_9$ и $\mathbb{F}_{11}$.

Упражнение. Покажите, что условие наличия единицы в этой задаче можно опустить, и это не повлияет на ответ. (Самое смешное, что условие коммутативности также можно опустить, это тоже не повлияет на ответ, но получится уже задача для аспирантов!)

Задача 2007–7

Имеется группа G и два взаимно простых числа m и n, такие, что $x^n y^n = y^n x^n$ и $x^m y^m = y^m x^m$ для любых $x, y \in G$. Докажите, что группа G абелева. (*Предложил А. Ю. Ольшанский.*)

Решение. Поскольку все n-е степени элементов из G коммутируют, они порождают абелеву подгруппу G^n, причем нормальную в G. Пусть G^m — абелева нормальная подгруппа, порожденная всеми m-ми степенями в G. Из-за взаимной простоты m и n найдутся целые u и v со свойством $um + vn = 1$. Поэтому $x = (x^u)^m (x^v)^n$ для всякого $x \in G$, то есть $G = G^m G^n$. Пересечение $Z = G^m \cap G^n$ лежит в центре группы G (коммутируя поэлементно как с G^m, так и с G^n). Оно содержит любой коммутатор $[g, h]$, где $g \in G^m$, $h \in G^n$. Поэтому факторгруппа G/Z, порожденная поэлементно перестановочными образами абелевых подгрупп G^m и G^n, абелева.

Для любых $x, y \in G$, преобразуем теперь $x^n y^n$, «перегоняя» игреки налево по одному, то есть заменяя каждый раз xy на равным ему yxz, где $z \in Z$, и отправляя каждый раз z в правый конец всего произведения, пользуясь его центральностью.

После n^2 шагов получим $y^n x^n z^{n^2}$. Поскольку $x^n y^n = y^n x^n$, мы получаем, что $z^{n^2} = 1$. Но точно так же $z^{m^2} = 1$. И так как n^2 и m^2 взаимно просты, $z = 1$. Значит $xy = yx$ для любых $x, y \in G$, что и требовалось доказать.

Упражнение. Покажите, что существует конечная неабелева группа, в которой все 2007-е степени элементов коммутируют между собой и все 99-е степени элементов коммутируют между собой; однако всякая конечная группа с этим свойством разрешима.

Задача 2007–8

Конечная группа действует на множестве так, что любой ее неединичный элемент имеет единственную неподвижную точку. Покажите, что эта точка одна и та же для всех элементов группы. (*Предложил А. А. Клячко.*)

Эту задачу мы позаимствовали из одной статьи[4] М. Форестера и К. Рурка, где она выступает в роли технической леммы.

Решение. Множество неединичных элементов группы G разбивается в объединение попарно непересекающихся стабилизаторов точек множества X:

$$G \setminus \{1\} = \coprod_{x \in X} (\mathrm{St}(x) \setminus \{1\}).$$

Множество неединичных стабилизаторов точек разбивается, в свою очередь, на классы сопряженных подгрупп. Другими словами, к одному классу относятся стабилизаторы точек одной орбиты. Число стабилизаторов в каждом таком классе совпадает с числом точек в соответствующей орбите Gx_i, то есть равно индексу стабилизатора $\mathrm{St}(x_i)$. Отсюда мы получаем:

$$|G| - 1 = \sum_{i=1}^{n} \frac{|G|}{|\mathrm{St}(x_i)|}(|\mathrm{St}(x_i)| - 1) = |G| \sum_{i=1}^{n} \left(1 - \frac{1}{|\mathrm{St}(x_i)|}\right),$$

где n — число орбит. Каждое ненулевое слагаемое в последней сумме не меньше $\frac{1}{2}$, поэтому число таких слагаемых не может быть больше единицы. Если все слагаемые нулевые, то группа тривиальна и доказывать нечего. Следовательно,

$$|G| - 1 = |G| \left(1 - \frac{1}{|\mathrm{St}(x_i)|}\right) = |G| - \frac{|G|}{|\mathrm{St}(x_i)|},$$

где i — номер единственного ненулевого слагаемого, и $G = \mathrm{St}(x_i)$, что и требовалось доказать.

Упражнение 1. Покажите, что условие конечности группы в этой задаче нельзя отбросить.

Упражнение 2. Существует ли конечная группа, которая раскладывается в объединение попарно тривиально пересекающихся собственных подгрупп, совпадающих со своими нормализаторами?

---

[4] Max Forester, Colin Rourke, "The adjunction problem over torsion-free groups", arXiv:math/0412274, Lemma 2.
См. также статью "A fixed point theorem and relative asphericity", Enseign. Math. 51 (2005), 231–237, Lemma 2.2.