Решения задач седьмой олимпиады по алгебре

Задача 1

Покажите, что квадратная матрица над полем вырождена тогда и только тогда, когда её можно разложить в произведение нескольких квадратных матриц, произведение которых в некотором другом порядке равно нулевой матрице. (*Предложил А. А. Клячко.*)

Решение. В одну сторону это очевидно: определитель произведения квадратных матриц равен произведению их определителей и потому не зависит от порядка сомножителей.

Докажем теперь, что всякую вырожденную матрицу A можно разложить в такое произведение. Элементарными преобразованиями строк и столбцов любую матрицу можно превратить в диагональную с нулями и единицами на диагонали. Матрица A вырождена, поэтому среди диагональных элементов полученной матрицы будет хотя бы один ноль, который, как нетрудно сообразить, можно поставить на любое диагональное место. Поскольку элементарные преобразования соответствуют умножению на невырожденные матрицы, мы имеем следующие разложения

$$A = P_1 A_1 Q_1 = \ldots = P_n A_n Q_n,$$

где матрицы P_i и Q_i невырождены, а A_i — диагональная матрица из нулей и единиц, причём i-й элемент её главной диагонали равен нулю. Так как $A_i^2 = A_i$, мы получаем

$$A = P_1 A_1 Q_1 = P_1 A_1^n Q_1 = P_1 \left(P_1^{-1} A Q_1^{-1}\right)^n Q_1 = P_1 \left(\prod_{i=1}^{n} P_1^{-1} P_i A_i Q_i Q_1^{-1}\right) Q_1.$$

Это произведение $(5n+2)$-х матриц после перестановки сомножителей становится нулевым, поскольку $\prod A_i = 0$.

Упражнение. Покажите, что любую вырожденную матрицу можно разложить в произведение нескольких матриц, произведение которых в *обратном* порядке нулевое.

Задача 2

Несколько студентов менялись шпаргалками. Произошло сто обменов «одну на одну», и в итоге все шпаргалки вернулись к своим первоначальным хозяевам. В скольких, максимум, руках могла побывать отдельно взятая шпаргалка? (*Предложил А. А. Клячко.*)

Ответ. У 51 студента, включая первоначального хозяина (то есть, в ста двух руках :).

Решение. Ясно, что указанная оценка достигается. Представьте себе, что студент A обменивает свою шпаргалку a на шпаргалку b студента B и сразу же совершает обратный обмен, потом обменивает ту же шпаргалку a на шпаргалку c студента C и сразу же совершает обратный обмен, и так далее. После ста обменов все шпаргалки окажутся у своих изначальных хозяев, причём шпаргалка a успеет побывать у пятидесяти одного студента.

Докажем теперь, что больше чем у пятидесяти одного студента никакой шпаргалке побывать не удастся. Нам будет удобнее доказывать чуть более общее утверждение: *если произошло l обменов и все шпаргалки вернулись к своим изначальным хозяевам, то никакая шпаргалка не могла побывать более чем у $(l/2+1)$-го студента.*

Если есть два студента, которые больше одного раза обмениваются, то этих двух студентов можно объединить в одного, тогда число обменов уменьшится по крайней мере на два (поскольку обмениваться самому с собой нет смысла), а число студентов, у которых побывала данная шпаргалка, уменьшится не больше чем на один. Это позволяет воспользоваться предположением индукции.

Осталось рассмотреть случай, когда никакие два студента не обмениваются больше одного раза. Но тогда каждая шпаргалка побывает не меньше чем у трёх студентов. Однако сумма длин путей, которые проходят все шпаргалки, равна удвоенному числу обменов. Значит, если какая-то шпаргалка побывает больше чем у s студентов, то

$$2l > s + 3(s-1), \quad \text{так как число шпаргалок не может быть меньше } s.$$

Откуда $s < (2l+3)/4 = l/2 + 3/4 < l/2 + 1$, что и требовалось.

Упражнение 1. Покажите, что в симметрической группе S_n разложение тождественной перестановки в произведение k (необязательно различных) транспозиций, порождающих S_n, единственно с

точностью до «некоммутативной перестановки сомножителей», то есть любые два таких разложения могут быть получены друг из друга конечным числом преобразований вида

$$e = t_1 \dots t_i t_{i+1} \dots t_k \;\longrightarrow\; e = t_1 \dots \underbrace{t_{i+1}}_{t'_i} \underbrace{(t_{i+1} t_i t_{i+1})}_{t'_{i+1}} \dots t_k \text{ и обратных к ним.}$$

Это теорема Клебша–Гурвица. О дальнейшем развитии этой темы и о применении таких вещей в алгебраической геометрии можно узнать из работ Вик. С. Куликова [Полугруппы разложений на множители и неприводимые компоненты пространства Гурвица. II, Изв. РАН. Сер. матем., 76:2 (2012), 151-160], см. также [http://arxiv.org/abs/1003.2953].

Задача 3

Докажите, что для любых элементов a и b конечной группы G число $|G| + \frac{|G|}{|\langle a\rangle|} + \frac{|G|}{|\langle b\rangle|} + \frac{|G|}{|\langle ab\rangle|}$ чётно. (*Предложил А. Е. Миронов.*)

Решение. Если порядок группы нечётный, то доказывать нечего.

Пусть $|G|$ чётно. Вложение G в $S_{|G|}$ по теореме Кэли переводит элемент g в произведение $\frac{|G|}{|\langle g\rangle|}$ независимых циклов длины $|\langle g\rangle|$. В частности, g даёт нечётную перестановку тогда и только тогда, когда $|G|$ чётно, а $\frac{|G|}{|\langle g\rangle|}$ нечётно.

Среди трёх перестановок a, b и ab либо ноль, либо две нечётных всегда. То есть, в рассматриваемой сумме либо ноль, либо два нечётных слагаемых (при чётном $|G|$).

Задача 4

Покажите, что для любого непустого подмножества X конечной группы G множество

$$X^{|G|} = \{x_1 x_2 \dots x_{|G|} \mid x_i \in X\}$$

является подгруппой. (*Автор неизвестен*[1].)

Решение. Приводимое ниже решение принадлежит Илье Богданову[2], мы его скопировали почти без изменений.

Мы утверждаем, что $|X^i| \leqslant |X^{i+1}|$ для всех натуральных i, причём если $|X^i| = |X^{i+1}|$, то $|X^{i+1}| = |X^{i+2}|$. Действительно, при отображении $X^i \times X \to X^{i+1}$, $(b, x) \mapsto bx$, полный прообраз любого элемента имеет мощность не больше $|X|$, так как все x-координаты элементов этого прообраза обязаны быть разными. Таким образом, $|X^i| \cdot |X| \leqslant |X^{i+1}| \cdot |X|$, то есть $|X^i| \leqslant |X^{i+1}|$, причём $|X^{i+1}| = |X^i|$ тогда и только тогда, когда полный прообраз любого элемента имеет мощность $|X|$, другими словами,

$$bxy^{-1} \in X^i \text{ для всех } b \in X^i \text{ и } x, y \in X.$$

Из этого вытекает, что $cxy^{-1} \in X^{i+1}$ для $c \in X^{i+1}$ и $x, y \in X$, стало быть $|X^{i+1}| = |X^{i+2}|$.

Если $|X^n| = n$ (где $n = |G|$) то $X^n = G$ и доказывать нечего. В противном случае $|X^i| = |X^{i+1}|$ для некоторого $i \leqslant n-1$ и, следовательно, $|X^i| = |X^{i+1}| = \dots = |X^n| = \dots = |X^{2n}|$. Поскольку $X^n \subseteq X^{2n}$ (так как $X^n \ni 1$), мы получаем, что X^n — подгруппа.

Упражнение (И. Богданов.)**.** Покажите, что $X^{|G|}$ является нормальной подгруппой в $\langle X\rangle$, причём факторгруппа является циклической. Покажите также, что равенство $|X^i| = |X^{i+1}|$ равносильно тому, что X^i является смежным классом группы $\langle X\rangle$ по подгруппе $X^{|G|}$.

---

[1] Мы взяли эту задачу с **Mathoverflow** (http://mathoverflow.net/questions/109590), куда её поместил(а) пользователь(ница) с псевдонимом *katie*. Однако комментаторы отмечают, что аналогичный вопрос почти одновременно появился на другом сайте, причём «авторы» не ссылаются ни друг на друга, ни куда-то ещё. Если кто-то знает первоисточник, сообщите нам об этом.

[2] http://mathoverflow.net/questions/109652.

Задача 5

Из двух многочленов со старшим коэффициентом один можно получить один и тот же путём возведения в степени ($f^k = g^l$) тогда и только тогда, когда их можно получить из одного и того же путём возведения в степени ($f = h^i$, $g = h^j$). При каких n в $\mathbb{Z}_n[x]$ это так для любых многочленов? (*Предложил А. А. Клячко.*)

Ответ. Это равносильно тому, что n не делится на квадраты натуральных чисел, больших единицы.

Решение. Если $n = p^k m$, где простое число p не делит m и $k \geqslant 2$, то $(x + p^{k-1}m)^p = x^p \pmod n$, так как все биномиальные коэффициенты C_p^k делятся на p при $0 < k < p$. Это доказывает утверждение в одну сторону, поскольку многочлены степени один $x + p^{k-1}m$ и x не могут, разумеется, быть получены из одного и того же путём возведения в степени. Действительно, если бы мы имели равенства $h^i = x$ и $h^j = x + p^{k-1}m$, то один из этих многочленов первой степени делился бы на другой, что явно не так.

Докажем теперь в другую сторону. Есть два многочлена f и g со старшим коэффициентом один и $f^k = g^l$. Надо показать, что найдётся такой многочлен h, что $f = h^i$ и $g = h^j$ при некоторых i и j.

Заметим, что для многочленов над полями это так в силу единственности разложения на неприводимые множители (со старшим коэффициентом один). Действительно, единственность разложения на неприводимые сводит утверждение к следующему простому факту: *если два целочисленных вектора линейно зависимы над $\mathbb{Q}$, то они могут быть получены из одного и того же целочисленного вектора умножением на целые числа* (докажите).

Похожая ситуация имеет место для многочленов над прямыми суммами полей, так как кольцо многочленов над прямой суммой изоморфно прямой сумме колец многочленов и всякий многочлен, у которого все координаты (многочлены над полями) имеют старший коэффициент один, единственным образом раскладывается в произведение многочленов, у которых одна из координат представляет собой неприводимый многочлен (над полем) со старшим коэффициентом один, а остальные координаты равны единице (докажите).

Осталось заметить, что по китайской теореме об остатках кольцо вычетов $\mathbb{Z}_n$ изоморфно прямой сумме полей $\left(\mathbb{Z}_n \simeq \bigoplus_{p|n} \mathbb{Z}_p\right)$, если число n не делится на квадраты.

Упражнение 1. Как изменится ответ, если убрать условие на старшие коэффициенты?

Упражнение 2. Какие многочлены над прямой суммой полей неприводимы?

Задача 6

Пусть V — линейное пространство, состоящее из нильпотентных матриц размера 3×3 над полем комплексных чисел. Может ли его (комплексная) размерность равняться а) 3, б) 4, в) 8? (*Предложили А. Э. Гутерман и О. В. Маркова.*)

Ответ. а) да, б) нет, в) нет.

Решение. Размерность 8 данное подпространство иметь не может: такую размерность имеет заведомо большее пространство матриц со следом 0.

Размерность 3 достигается на пространстве $\mathcal{T} = \langle E_{1,2}, E_{1,3}, E_{2,3}\rangle$.

Докажем, что наибольшая размерность подпространства V комплексных нильпотентных матриц размера 3×3 равна 3.

1. Если матрица A нильпотентна, то ее след равен 0.
2. $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.
3. Если матрицы A, B и $A + B$ нильпотентны, то $\operatorname{tr}(AB) = 0$.
   Действительно, $AB+BA = (A+B)^2-A^2-B^2$, откуда $2\operatorname{tr}(AB) = \operatorname{tr}((A+B)^2)-\operatorname{tr}(A^2)-\operatorname{tr}(B^2) = 0$ и $\operatorname{tr}(AB) = 0$.
4. Существует разложение $V = V_1 \oplus V_2$, где $V_1 = V \cap \mathcal{T}$.
5. $\operatorname{tr}(AB)$ — невырожденная симметрическая билинейная функция ($\operatorname{tr}(AE_{i,j}) = a_{j,i}$) на $M_3(\mathbb{C})$.
6. Для произвольного подпространства $\mathcal{L} \subseteq M_3(\mathbb{C})$ обозначим
   $$\mathcal{L}^\perp = \{A \in M_3(\mathbb{C}) : \operatorname{tr}(AB) = 0 \ \forall B \in \mathcal{L}\}.$$
   Тогда $\dim \mathcal{L} + \dim \mathcal{L}^\perp = \dim M_3(\mathbb{C}) = 9$.
7. Непосредственно (из 5) вычисляется, что $\mathcal{T}^\perp = \langle E_{1,1}, E_{1,2}, E_{1,3}, E_{2,2}, E_{2,3}, E_{3,3}\rangle$.
8. $V_2 \cap \mathcal{T}^\perp = \{0\}$.

9. Для любых матриц $A \in V_1, B \in V_2, C \in \mathcal{T}^\perp$ имеем $\operatorname{tr}(AB) = 0$ по доказанному в 3 и $\operatorname{tr}(AC) = 0$, поскольку $V_2 \subseteq \mathcal{T}$, откуда $B + C \in V_1^\perp$ и в силу произвольности их выбора $V_2 \oplus \mathcal{T}^\perp \subseteq V_1^\perp$.
10. Тогда $\dim V_2 + 6 = \dim V_2 + \dim \mathcal{T}^\perp \leqslant \dim V_1^\perp = 9 - \dim V_1$, откуда $\dim V = \dim V_1 + \dim V_2 \leqslant 9 - 6 = 3$.

В общем случае размерность пространства V ограничена числом $\frac{n(n-1)}{2}$, где n — порядок матриц. Для полей характеристики, не равной 2, доказательство точно такое же а общий случай можно найти в [Ben Mathes, Matjaž Omladic, Heydar Radjavi, Linear spaces of nilpotent matrices, Linear Algebra Appl., 1991, V. 149, P 215–225.]

Задача 7

Пусть A — ассоциативное коммутативное кольцо с единицей, в котором $a + a = 0$ и $a^2 = a$ для всех $a \in A$, и M — матрица размера $n \times n$ над этим кольцом, определитель которой равен 1. Докажите, что матрица M имеет конечный порядок (то есть, $M^k = E$ для некоторого натурального k). (*Предложил В. А. Брагин.*)

Решение. Пусть $b_1, b_2, \dots b_{n^2}$ — элементы матрицы. Тогда заметим, что подкольцо R, порождённое ими, состоит из всевозможных многочленов от них. Но всего различных одночленов 2^{n^2} (каждая переменная в степени 0 или 1), а коэффициент перед одночленом также либо 0, либо 1. Поэтому многочленов всего конечное число. То есть $d = |R| < 2^{2^{n^2}}$.

Очевидно, что элементы степеней M лежат в R, поэтому среди степеней M не более d^{n^2} различных. Отсюда следует, что $M^k = M^l$ для некоторых $k > l$. А поскольку M обратима, то $M^{k-l} = E$.

Упражнение. Покажите, что условие коммутативности можно опустить, так как оно автоматически будет следовать из других условий.

Задача 8

Покажите, что никакой автоморфизм неабелевой конечной группы не может больше трёх четвертей элементов группы переводить в обратные к ним элементы. (*Предложил А. А. Клячко*[3].)

Решение. Приводимое ниже доказательство принадлежит П. Р. Солису[4].

Предположим, что автоморфизм f группы G переводит более трёх четвертей её элементов в обратные. Пусть $H = \{x \in G \mid f(x) = x^{-1}\}$. Тогда $|H| > \frac{3}{4}|G|$ и, следовательно, $|H \cap hH| > \frac{1}{2}|G|$ для любого $h \in H$. Но включения $h, x, hx \in H$ означают, что

$$f(hx) = f(h)f(x) = h^{-1}x^{-1}, \text{ а с другой стороны, } f(hx) = (hx)^{-1} = x^{-1}h^{-1},$$

то есть любой элемент $h \in H$ коммутирует более чем с половиной элементов группы G, а значит и со всеми элементами по теореме Лагранжа, так как централизатор элемента h — это подгруппа. Осталось заметить, что подгруппа, порождённая множеством H, совпадает со всей группой G опять же по теореме Лагранжа. Таким образом, все элементы группы G коммутируют между собой, что и требовалось.

Упражнение. Покажите, что имеется бесконечно много неабелевых групп, обладающих автоморфизмом, переводящим ровно три четверти элементов в обратные, и все такие группы разрешимы.

---

[3] наткнувшийся на этот вопрос на **Mathoverflow** (http://mathoverflow.net/questions/38), но факт известен давно, см. работу Дж. А. Миллера 1929 года [Proc. NAS 15:369–372].

[4] http://mathoverflow.net/questions/48.