Задача 2006–1

Элементов какого порядка в группе $\mathbf{S}_n$ больше: четного или нечетного? (*Предложил А. Э. Гутерман.*)

Решение. При $n = 2, 3$ легко убедиться, что подстановок четного и нечетного порядка одинаковое число. Пусть $n \geqslant 4$. Заметим, что все нечетные подстановки имеют четный порядок: действительно, нечетная подстановка в нечетной степени нечетна, следовательно, не может быть равна тождественной – четной подстановке. Кроме того, существуют четные подстановки четного порядка, например, (12)(34). Так как четных и нечетных подстановок одинаковое количество, отсюда следует, что при $n \geqslant 4$ подстановок четного порядка больше.

Упражнение. Каких подстановок в $\mathbf{S}_n$ больше: являющихся квадратами или не являющихся квадратами?

Задача 2006–2

Студенту Д. задали на дом решить все системы из пяти линейных уравнений с пятью неизвестными над полем из пяти элементов (всего 5^{30} систем). Сколько из этих систем является совместными? Сколько является определенными? (*Предложил А. А. Клячко.*)

Решение. Пусть

b_k — число упорядоченных наборов из k линейно независимых векторов в $\mathbb{Z}_5^5$;
b'_k — число упорядоченных наборов из k линейно независимых векторов в $\mathbb{Z}_5^k$;
p_k — число подпространств размерности k в $\mathbb{Z}_5^5$;
R_V — число матриц в $M_5(\mathbb{Z}_5)$, у которых линейная оболочка столбцов порождает подпространство V в $\mathbb{Z}_5^5$;
r_k — число матриц ранга k в $M_5(\mathbb{Z}_5)$;
s_k — число совместных систем, ранга k, из пяти линейных уравнений с пятью неизвестными над $\mathbb{Z}_5$.

Тогда

$$b_k = \prod_{i=0}^{k-1} (5^5 - 5^i).$$

(Здесь и везде произведение пустого множества сомножителей считается равным единице.)

В самом деле, первый вектор линейно независимого набора может быть любым ненулевым вектором ($5^5 - 1$ возможность); второй вектор (при фиксированном ненулевом первом векторе) может быть любым, неколинеарным первому, ($5^5 - 5$ возможностей); и т.д.

Аналогично,

$$b'_k = \prod_{i=0}^{k-1} (5^k - 5^i).$$

Подпространство размерности k в $\mathbb{Z}_5^5$ однозначно определяется своим базисом, а различных базисов в каждом таком пространстве b'_k штук. Поэтому $p_k = \frac{b_k}{b'_k}$. (Обратите внимание на двойственность: $p_k = p_{5-k}$. Вы можете доказать это из «общих соображений»?)

Ясно, что величина R_V зависит только от размерности пространства V. Поэтому, выбирая в качестве V линейную оболочку первых k векторов стандартного базиса $\mathbb{Z}_5^5$, мы получаем, что R_V есть число матриц, у которых первые $k = \dim V$ строк линейно независимы, а остальные строки нулевые. То есть,

$$R_V = b_{\dim V}.$$

Следовательно,

$$r_k = p_k b_k.$$

Кроме того, система, матрица коэффициентов которой имеет ранг k, совместна тогда и только тогда, когда столбец свободных членов лежит в линейной оболочке столбцов матрицы коэффициентов, то есть для выбора свободных членов мы имеем 5^k возможностей. Следовательно,

$$s_k = 5^k r_k.$$

Все суммируя и подставляя, мы получаем **ответ**:

число совместных систем $= \sum\limits_{k=0}^{5} s_k = \sum\limits_{k=0}^{5} \prod\limits_{i=0}^{k-1} \frac{5(5^5-5^i)^2}{(5^k-5^i)}$;

число определенных систем $= s_5 = 5^5|\mathbf{GL}_5(\mathbb{Z}_5)| = 5^5 \prod\limits_{i=0}^{4}(5^5-5^i)$.

Задача 2006–3

Пусть F — поле, $M_n(F)$ — пространство матриц размера $n\times n$ над F, $T : M_n(F) \to M_n(F)$ — линейное отображение, такое, что $\det(A) = \det(T(A))$ для любой $A \in M_n(F)$. Докажите, что отображение T обратимо. (*Предложил А. Э. Гутерман*[1].)

Решение. Предположим, что существует матрица $A \neq 0$, для которой $T(A) = 0$. Так как $\det(A) = \det(T(A)) = \det(0) = 0$, имеем: A — вырожденная матрица. Пусть $r = \mathrm{rk}(A)$ — ранг матрицы A. Тогда существует такая матрица B, что $A+B$ — невырожденная матрица и $\mathrm{rk}(B) = n-r < n$. Следовательно, $\det(T(B)) = \det(B) = 0$. Отсюда имеем:

$$0 = \det(T(B)) = \det(T(B) + T(A)) = \det(T(B + A)) = \det(B + A) \neq 0$$

— противоречие. Тем самым, линейный оператор T на конечномерном пространстве инъективен, а значит, обратим.

Упражнение 1. Попробуйте доказать следующую теорему Фробениуса: *для любого линейного отображения T из пространства квадратных комплексных матриц в себя, сохраняющего определитель, найдутся такие матрицы A и B, что либо $T(X) = AXB$ для любой матрицы X, либо $T(X) = AX^\top B$ для любой матрицы X.*

Упражнение 2. Докажите, что если линейное отображение сохраняет определитель, то оно сохраняет ранг.

Упражнение 3. Докажите, что если обратимый линейный оператор на пространстве матриц над алгебраически замкнутым полем переводит в себя алгебраическое множество S (т. е. множество, задаваемое в виде нулей некоторой системы полиномиальных уравнений), то этот оператор биективен на множестве S.

Упражнение 4. Приведите пример необратимого линейного оператора на множестве вещественных матриц, переводящего обратимые матрицы в обратимые.

Задача 2006–4

Студент Д. называет квадратную вещественную матрицу A *практически обратимой*, если найдется такая матрица B, что элементы матрицы $C = AB$ отличаются от соответствующих элементов единичной матрицы не более чем на 10^{-10}:

$$|c_{ij} - \delta_{ij}| \leqslant \frac{1}{10000000000} \quad \text{для всех } i, j.$$

Существуют ли практически обратимые необратимые матрицы? (*Предложил А. А. Клячко.*)

Решение. Да, существуют. Матрица

$$A = E - 10^{-10} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1 \end{pmatrix}$$

размера $10^{10} \times 10^{10}$ практически обратима (в качестве «практически обратной» матрицы B можно взять единичную матрицу), но не обратима, потому что вырождена — сумма строк равна нулю.

Упражнение. Покажите, что всякая практически обратимая матрица размера меньшего чем 10^{10} является обратимой.

---

[1] См. также статью M. Marcus, B. Moyls, "Linear transformations on algebras of matrices", Can. J. Math, vol. 11 (1959a) 61–66.

Задача 2006–5

Пусть $f(x_1, \ldots, x_n)$ — однородный многочлен степени k с комплексными коэффициентами. Докажите, что для некоторого натурального m найдутся такие линейные многочлены $L_j = \sum_{i=1}^{n} a_{ij} x_i$, $j = 1, \ldots, m$, $a_{ij} \in \mathbb{C}$, что

$$f(x_1, \ldots, x_n) = L_1^k + \cdots + L_m^k.$$

(*Предложил И. В. Аржанцев.*)

Решение. Рассмотрим случай $n = 2$. Вычисляя коэффициенты при помощи бинома Ньютона и используя определитель Вандермонда, легко показать, что многочлены $x_1^k, (x_1 + x_2)^k, \ldots, (x_1 + kx_2)^k$ линейно независимы и, следовательно, образуют базис пространства однородных многочленов степени k от переменных x_1 и x_2. Это означает, что для произвольного однородного многочлена $f(x_1, x_2)$ степени k найдутся такие комплексные числа $\alpha_0, \ldots, \alpha_k$, что

$$f(x_1, x_2) = \alpha_0 x_1^k + \cdots + \alpha_k (x_1 + kx_2)^k = (\beta_0 x_1)^k + \cdots + (\beta_k (x_1 + kx_2))^k,$$

где $\beta_i^k = \alpha_i$.

Для $n > 2$ будем вести индукцию по n. Достаточно доказать, что любой одночлен $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ степени k представим в нужном нам виде. Можно считать, что $i_1 \geqslant 1$. По предположению индукции одночлен $x_2^{i_2} \ldots x_n^{i_n}$ представим в виде $S_1^{k-i_1} + \cdots + S_m^{k-i_1}$, где S_j — линейные многочлены от $x_2, \ldots, x_n$. Остается заметить, что, вновь по предположению индукции, многочлен $x_1^{i_1} S_j^{k-i_1}$ представим в виде суммы k-х степеней линейных многочленов от x_1 и S_j.

Упражнение. Найдите верхнюю оценку на число слагаемых m.

Замечание. Эту задачу можно рассматривать как алгебраическую версию проблемы Варинга из теории чисел[2]. Последняя утверждает, что каждое натуральное число можно представить в виде суммы k слагаемых, каждое из которых является n-й степенью целого неотрицательного числа, причем число k зависит только от n. Частным случаем этого утверждения является теорема Лагранжа о представимости чисел в виде суммы четырех квадратов.

Задача 2006–6

Студент Д. называет поле *практически алгебраически замкнутым*, если в этом поле каждый многочлен положительной степени, не превосходящей 10000000000, имеет корень. Может ли практически алгебраически замкнутое поле

а) быть конечным?

б) не быть алгебраически замкнутым?

(*Предложил А. А. Клячко.*)

Решение. Конечным практически алгебраически замкнутое поле F быть не может. Действительно, рассмотрим многочлен $f(x) = x^2 - x$. Этот многочлен переводит два элемента в один: $f(0) = f(1)$. Следовательно, в случае конечного поля в некоторый элемент $c \in F$ не переходит ничего: $c \notin f(F)$. То есть, квадратный многочлен $f(x) - c$ не имеет корней и поле не является практически алгебраически замкнутым. На самом деле, почти в любом учебнике по алгебре доказывается, что над каждым конечным полем имеется неприводимый многочлен любой положительной степени.

Построим теперь практически алгебраически замкнутое поле, не являющееся алгебраически замкнутым. Возьмем простое число $p > 10000000000$ (приведите пример такого числа[3]!). Рассмотрим максимальное (по включению) подполе[4] P поля комплексных чисел, содержащее число π и все корни степени p из единицы, но не содержащее $\sqrt[p]{\pi}$. Символом π мы здесь обозначаем произвольное трансцендентное число (например, отношение длины окружности к ее диаметру).

Многочлен $f(x) = x^p - \pi$ является неприводимым над полем P. Действительно, над полем комплексных чисел многочлен f раскладывается как:

$$f(x) = (x - \sqrt[p]{\pi})(x - \varepsilon \sqrt[p]{\pi})(x - \varepsilon^2 \sqrt[p]{\pi}) \ldots (x - \varepsilon^{p-1} \sqrt[p]{\pi}),$$

где ε — первообразный корень степени p из единицы.

---

[2] См., например, книгу А. Я. Хинчина «Три жемчужины теории чисел», 2 изд., М. — Л., 1948.

[3] Это шутка.

[4] Существование такого максимального подполя кажется очевидным, но чтобы это строго доказать нужна аксиома выбора (точнее говоря, это немедленно вытекает из леммы Цорна).

Следовательно, приводимость многочлена f над полем P:

$$x^p - \pi = (x^k + a_1 x^{k-1} + \dots)(x^{p-k} + \dots), \quad \text{где } 0 < k < p,$$

означает (по теореме Виета), что сумма нескольких, но не всех корней многочлена f лежит в P:

$$\sqrt[p]{\pi} \sum_{j=1}^{k} \varepsilon^{s_j} = -a_1 \in P.$$

То есть,

$$\text{либо } \sqrt[p]{\pi} \in P, \quad \text{либо } \sum_{j=1}^{k} \varepsilon^{s_j} = 0.$$

Первое не может быть верным по определению поля P, а второе просто неверно: *сумма нескольких, но не всех, корней из единицы простой степени p не может равняться нулю.* (Докажите!) Полученное противоречие показывает, что многочлен f неприводим над P. Другими словами, числа

$$1, \sqrt[p]{\pi}, \sqrt[p]{\pi^2}, \dots, \sqrt[p]{\pi^{p-1}}$$

линейно независимы над P.

Докажем, что поле P является практически алгебраически замкнутым. Рассмотрим поле P', получающееся из P присоединением корня некоторого неприводимого многочлена маленькой степени (не превосходящей 10000000000). Размерность поля P', как векторного пространства над P, не превосходит 10000000000. Следовательно, $\sqrt[p]{\pi} \notin P'$ (в силу линейной независимости чисел $1, \sqrt[p]{\pi}, \sqrt[p]{\pi^2}, \dots, \sqrt[p]{\pi^{p-1}}$). Значит $P' = P$ по свойству максимальности поля P. Мы видим, что поле P является практически алгебраически замкнутым, но не является алгебраически замкнутым.

Упражнение. Существует ли практически алгебраически замкнутое, но не алгебраически замкнутое поле положительной характеристики?

Задача 2006–7

Пусть конечная группа G транзитивно действует на конечном множестве X, содержащем более одного элемента. Может ли каждый элемент группы G иметь в X неподвижную точку? (*Предложил Ю. Г. Прохоров*[5].)

Решение. Допустим, что может. Порядок орбиты равен индексу стабилизатора, поэтому $|G| = |X| \cdot |\operatorname{St}(x_0)|$, где $x_0 \in X$ — любая точка.

С другой стороны, по предположению $G = \bigcup\limits_{x \in X} \operatorname{St}(x)$ и, следовательно,

$$|G| < \sum_{x \in X} |\operatorname{St}(x)| = |X| \cdot |\operatorname{St}(x_0)|$$

(неравенство строгое, так как единица лежит во всех стабилизаторах). Получили противоречие.

Замечание. Решение задачи также следует из формулы Бернсайда[6].

Упражнение. Докажите, что никакая конечная группа не может быть разложена в объединение собственных сопряженных между собой подгрупп.

Задача 2006–8

Для каких натуральных n существует группа из n элементов, у которой ровно четыре силовские (неединичные) подгруппы? (*Предложила Е. И. Бунина.*)

Решение. Пусть $n = p_1^{k_1} p_2^{k_2} \dots p_l^{k_l}$ – разложение числа n на простые множители. Тогда $l \leqslant 4$, так как каждому простому делителю отвечает не менее одной силовской подгруппы.

Если $l = 1$, то мы имеем p-группу, у нее всего одна силовская подгруппа.

Пусть $l = 2$. Тогда $n = p_1^{k_1} p_2^{k_2}$, есть три силовские p_1-подгруппы и одна силовская p_2-подгруппа. Значит, 3 сравнимо с единицей по модулю p_1, откуда $p_1 = 2$. Далее, 3 делит $p_2^{k_2}$, откуда $p_2 = 3$. Остается заметить, что группа

$$S_3 \times \mathbb{Z}_{2^{k_1-1}} \times \mathbb{Z}_{3^{k_2-1}}$$

[5]См. Rose, J. S. (1978) A course on group theory. Cambridge UK: Cambridge University Press.

[6]См., например, книгу Э. Б. Винберга «Курс алгебры», М.: МЦНМО (2011).

имеет три силовские 2-подгруппы и одну силовскую 3-подгруппу.

Если $l = 3$, то для некоторого i существует ровно две силовские p_i-подгруппы, однако число 2 не сравнимо с единицей по модулю p_i.

Наконец, для $l = 4$ в качестве G можно взять абелеву группу порядка n.

Ответ. $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} p_4^{k_4}$ или $n = 2^{k_1} 3^{k_2}$, где p_1, p_2, p_3, p_4 — различные простые, а k_1, k_2, k_3, k_4 — натуральные числа.

Упражнение 1. Решите аналогичную задачу для случая пяти силовских подгрупп.

Упражнение 2. Для каких натуральных n существует группа из n элементов, у которой ровно четыре подгруппы, порядки которых — степени (возможно, разных) простых чисел?