Уравновешенные разложения на множители в некоторых алгебрах

А. А. Клячко, А. М. Мажуга, А. Н. Понфиленко

Мы доказываем, что во всяком поле характеристики не два и не три, кроме $\mathbb{F}_5$, каждый элемент раскладывается в произведение четырёх множителей, сумма которых равна нулю. Мы также находим все такие k, n, q, что каждая матрица размера $n \times n$ над полем из q элементов раскладывается в произведение k коммутирующих матриц с нулевой суммой.

§ 0. Введение

Покажите, что всякое рациональное число можно разложить в произведение нескольких рациональных чисел, сумма которых равна нулю.

Эта задача предлагалась на Казахстанской республиканской олимпиаде для школьников в 2013 году [1]. Аналогичный вопрос для произвольного поля характеристики не два предлагался на студенческой олимпиаде по алгебре в МГУ в 2014 году [2]. Задача рассматривалась и раньше [3] (также в контексте работы со способными школьниками).

Вопрос о наличии таких *уравновешенных* или *сбалансированных* разложений (то есть разложений в произведение нескольких множителей, сумма которых равна нулю) решается легко в любом поле характеристики не два. Гораздо труднее выяснить, сколько множителей могут содержать такие уравновешенные разложения. На самом деле (см. [4]),

в любом поле характеристики не два каждый элемент допускает уравновешенное разложение в произведение k сомножителей для каждого $k \geqslant 5$. (А для каждого $k < 5$ найдётся поле, в котором это утверждение перестаёт быть верным.)

При $k < 5$ вопрос становится более тонким, например, в поле рациональных чисел не всякий элемент допускает уравновешенное разложение

Первые два автора поддержаны РФФИ, грант № 15–01–05823.

в произведение трёх множителей [3], а вопрос о четырёх множителях оставался открытым. В [3] приводится следующее электронное письмо М. А. Цфасмана А. В. Иванищуку:

$$3 = (363/70) \cdot (20/77) \cdot (-49/110) \cdot (-5). \quad \text{Уф...} \qquad \text{Ваш М. А.}$$

Это письмо содержит (первое открытое) уравновешенное разложение тройки в произведение четырёх множителей в поле рациональных чисел. Аналогичные разложения для единицы и двойки выглядят не так впечатляюще: $1{=}1{\cdot}1{\cdot}(-1){\cdot}(-1)$ и $2{=}(1/6){\cdot}(9/2){\cdot}(-2/3){\cdot}(-4)$. Статья [3] содержит полученные с помощью компьютера уравновешенные разложения первых пятидесяти натуральных чисел в произведение четырёх рациональных множителей.

Мы доказываем, что любое рациональное число допускает уравновешенное разложение в произведение четырёх рациональных сомножителей. Более того, имеет место следующая теорема, отвечающая на два вопроса из [4] (один из них был поставлен раньше [3]).

Теорема 1. *Во всяком поле характеристики не два и не три, кроме пятиэлементного поля* $\mathbb{F}_5$, *каждый элемент допускает уравновешенное разложение в произведение четырёх множителей; если это поле бесконечно, то каждый элемент допускает бесконечно много таких разложений.*

По поводу этого результата мы не уверены в своём приоритете, поскольку

— школьный учитель второго автора, Дмитрий Витальевич Андреев, много лет назад (в 2003 году) предлагал такую задачу на уроке (для случая поля рациональных чисел); задача не была решена, но из данных учителем подсказок второй автор (теперь, уже зная решение) склонен делать вывод, что Дмитрий Витальевич умел решать эту задачу;
— в 2016 году, уже зная решение, второй автор задал такой вопрос (для случая рациональных чисел) на форуме `http://math.stackexchange.com/` и вскоре кто-то из посетителей этого форума предоставил решение, отличающееся от нашего, но, вероятно, тоже правильное; сейчас этот вопрос, к сожалению, удалён, и мы не можем дать никакой более точной ссылки.

Следующая теорема из [4] описывает для каждого k все конечные поля, в которых каждый элемент допускает уравновешенное разложение в произведение k множителей.

Теорема об уравновешенных разложениях в конечных полях [4]. *Пусть* $k \geqslant 2$ *— целое число и* F *— конечное поле. В поле* F *всякий элемент можно разложить в произведение* k *сомножителей, сумма которых равна нулю, тогда и только тогда, когда* (см. табл. 1) *либо* $|F| = 2$ *и* k *чётно, либо* $|F| = 4$ *и* $k \neq 3$, *либо* $|F|$ *— степень двойки, но не двойка и не четвёрка* *(и k любое), либо $|F| \in \{3, 5\}$ и $k \notin \{2, 4\}$, либо $|F| = 7$ и $k \notin \{2, 3\}$, либо $|F|$ не степень двойки, не три, не пять и не семь и $k \neq 2$.*

Таблица 1

Наличие уравновешенного разложения в конечных полях

	$k=2$	$k=3$	$k=4$	$k=5,7,9,\ldots$	$k=6,8,10,\ldots$
$\mathbb{F}_2$	да	нет	да	нет	да
$\mathbb{F}_3$	нет	да	нет	да	да
$\mathbb{F}_4$	да	нет	да	да	да
$\mathbb{F}_5$	нет	да	нет	да	да
$\mathbb{F}_7$	нет	нет	да	да	да
$\mathbb{F}_8, \mathbb{F}_{16}, \mathbb{F}_{32}, \mathbb{F}_{64}, \ldots$	да	да	да	да	да
$\mathbb{F}_9, \mathbb{F}_{11}, \mathbb{F}_{13}, \mathbb{F}_{17}, \ldots$	нет	да	да	да	да

Следующая теорема дополняет этот результат из [4], см. табл. 2.

Теорема 2. *Пусть $k, n \geqslant 2$ — целые числа и F — конечное поле. Каждая матрица $n \times n$ над полем F раскладывается в произведение k коммутирующих матриц, сумма которых равна нулю, тогда и только тогда, когда либо $k = 3$ и $|F| = 5$, либо $k = 3$ и $|F| \geqslant 8$, либо $k = 4$ и $|F| = 4$, либо $k = 4$ и $|F| \geqslant 7$, либо $k \geqslant 5$ и $|F| \geqslant 3$.*

Другими словами, ситуация в матричных алгебрах над конечными полями такая (на верхние индексы пока не нужно обращать внимание):

Таблица 2

Наличие уравновешенного разложения в матричных алгебрах над конечным полем

	$k=2$	$k=3$	$k=4$	$k=5,6,7,8,\ldots$
$\mathbb{F}_2$	нет^1	нет^0	нет^2	нет^2
$\mathbb{F}_3$	нет^1	нет^8	нет^0	да^{3,4}
$\mathbb{F}_4, \mathbb{F}_7$	нет^1	нет^0	да^{5,7}	да^{3,4,5,7}
$\mathbb{F}_5$	нет^1	да^5	нет^0	да^{3,4}
$\mathbb{F}_8, \mathbb{F}_9, \mathbb{F}_{11}, \mathbb{F}_{13}, \mathbb{F}_{16}, \ldots$	нет^1	да^{5,6}	да^{5,7}	да^{3,4,5,7}

Обратите внимание, что от размера матриц ответ не зависит, если этот размер по крайней мере 2.

В первом параграфе мы доказываем теорему 1 и ещё одну теорему о конечных полях (теорема 3), которая играет ключевую роль в доказательстве теоремы 2. Все рассуждения первого параграфа вполне элементарны, за исключением того, что доказательство теоремы 3 существенно опирается на результаты работы [4] (которые, в свою очередь, опираются на теорию эллиптических кривых). Во втором параграфе мы доказываем теорему 2.

Обозначения, которые мы используем, в целом стандартны. Отметим только, что символ $\mathbb{F}_q$ обозначает поле из q элементов, а буква E обозначает единичную матрицу.

§ 1. Поля

Доказательство теоремы 1. Имеет место тождество

$$x = \frac{2(1-4x)^2}{3(1+8x)} \cdot \frac{-(1+8x)}{6} \cdot \frac{-(1+8x)}{2(1-4x)} \cdot \frac{18x}{(1-4x)(1+8x)}.$$

Мы можем только предложить читателю проверить непосредственно это тождество и тот факт, что сумма множителей равна нулю. В исключительных случаях, когда знаменатели обращаются в нуль, т. е. при $x \in \{1/4, -1/8\}$, следует умножить x на y^4, подобрав y так, что $xy^4 \notin \{1/4, -1/8, 0\}$ (в любом поле характеристики не два и не три, кроме $\mathbb{F}_5$, это заведомо возможно), написать аналогичное разложение для xy^4 и потом разделить каждый сомножитель на y:

$$x = \frac{2(1-4xy^4)^2}{3y(1+8xy^4)} \cdot \frac{-(1+8xy^4)}{6y} \cdot \frac{-(1+8xy^4)}{2y(1-4xy^4)} \cdot \frac{18xy^4}{y(1-4xy^4)(1+8xy^4)}.$$

Таким образом, мы получаем уравновешенное разложение любого элемента в произведение четырёх множителей. Бесконечность числа таких разложений в случае бесконечного поля вытекает из последнего тождества и следующего элементарного факта, доказательство которого мы оставляем читателям в качестве упражнения:

> не равная константе рациональная дробь над бесконечным полем принимает бесконечное число значений.

(Отметим, что, например, второй сомножитель в последнем тождестве при каждом x представляет собой не равную константе рациональную дробь $f(y)$.) Это завершает доказательство теоремы. Поле из пяти элементов действительно является исключением, как видно из табл. 1. $\square$

Аналогично можно получить бесконечно много уравновешенных разложений в произведение любого большего числа сомножителей, то есть

> в любом бесконечном поле характеристики не два каждый элемент допускает бесконечно много уравновешенных разложений в произведение k сомножителей для каждого $k \geqslant 5$.

Например, следующее тождество получается лёгкой модификацией из тождества, приведённого в [4], и даёт бесконечно много уравновешенных разложений произвольного ненулевого элемента бесконечного поля характеристики не два в произведение 2017 сомножителей:

$$x = \frac{xy^{2016}}{2} \cdot \frac{xy^{2016}}{2} \cdot (-xy^{2016}) \cdot \frac{2}{xy^{2018}} \cdot \left(-\frac{2}{xy^{2018}}\right) \cdot \left(\frac{1}{y}\right)^{1006} \cdot \left(-\frac{1}{y}\right)^{1006}.$$

Разложение на множители $x = x_1x_2 \dots x_k$ называется *степенны́м*, если все сомножители равны друг другу: $x_1 = \dots = x_k$ [4].

Теорема 3. *Пусть $k \geqslant 2$ — целое число и F — конечное поле. В поле F всякий элемент допускает нестепенное уравновешенное разложение в произведение k множителей тогда и только тогда, когда либо $k = 3$ и $|F| = 5$, либо $k = 3$ и $|F| \geqslant 8$, либо $k = 4$ и $|F| = 4$, либо $k = 4$ и $|F| \geqslant 7$, либо $k \geqslant 5$ и $|F| \geqslant 3$.*

Другими словами, ответ здесь такой же, как в теореме 2 (табл. 2).

Доказательство. Верхние индексы у частиц *да* и *нет* в табл. 2 соответствуют случаям из доказательства ниже.

Случай 0: нет, так как тогда у некоторых элементов нет никаких сбалансированных разложений (по теореме об уравновешенных разложениях в конечных полях).

Случай 1: $k = 2$ — нет. Для любого элемента a рассмотрим его уравновешенное разложение $a = xy$, $x + y = 0$. Если у поля характеристика 2, то наше разложение $a = (-x)x$ является степенным; если же характеристика конечного поля не два, то не всякий элемент является квадратом и, следовательно, не всякий элемент допускает уравновешенное разложение в произведение двух множителей.

Случай 2: $|F| = 2$ — нет. В разложении единицы могут участвовать только единицы, поэтому оно будет степенным.

Случай 3: $k = 5 + 2n$, где $n \geqslant 0$ и $\operatorname{char} F \neq 2$ — да. Здесь можно использовать универсальную формулу для уравновешенных разложений в произведение $5 + 2n$ сомножителей из [4]:

$$\pm a = (-a) \cdot \frac{a}{2} \cdot \frac{a}{2} \cdot \frac{2}{a} \cdot \frac{-2}{a} \cdot 1^n \cdot (-1)^n \quad (\text{при } a \neq 0).$$

При этом $\operatorname{char} F \neq 2$, поэтому $\frac{2}{a} \neq -\frac{2}{a}$ и, значит, это разложение нестепенное. А нулевой элемент очевидно имеет уравновешенное нестепенное разложение: $0 = (-1) \cdot 1 \cdot 0^{k-2}$.

Случай 4: $k = 6 + 2n$, где $n \geqslant 0$ и $\operatorname{char} F \neq 2$ — да. Воспользуемся общей формулой для уравновешенных разложений в произведение $6 + 2n$ множителей из [4]. Рассмотрим такое ненулевое $c \in F$, что $c^2 \neq a$ (такое c всегда найдётся, кроме случая, когда $F = \mathbb{F}_3$ и $a = 1$; но тогда всё очевидно).

Положим $b = (c^2 - a)/c$. Тогда
$$\pm a = (-c) \cdot (c - b) \cdot \frac{b}{2} \cdot \frac{b}{2} \cdot \frac{2}{b} \cdot \frac{-2}{b} \cdot 1^n \cdot (-1)^n.$$
Так как $\operatorname{char} F \neq 2$, мы имеем $\frac{2}{b} \neq -\frac{2}{b}$, поэтому разложение нестепенное.

Случай 5: $|F| = 5, 8$ и $k = 3$; $|F| = 7, 9, \ldots$ и $k = 4$; $|F| = 4, 8$ и $k = 5 + 2n$, где $n \geqslant 0$. В этом случае уравновешенное разложение существует по теореме об уравновешенных разложениях в конечных полях и не может быть степенным, поскольку число сомножителей не делится на характеристику поля, а их сумма равна нулю.

Случай 6: $|F| \geqslant 9$, $\operatorname{char} F \neq 2$ и $k = 3$ — да.

Здесь нужно рассмотреть два случая. Если $\operatorname{char} F \neq 3$, то по теореме об уравновешенных разложениях в конечных полях уравновешенное разложение у любого элемента существует, а так как $\operatorname{char} F \neq 3$, то оно заведомо нестепенное.

Для доказательства в случае характеристики три нам понадобится вспомогательное утверждение.

Лемма. *В поле $\mathbb{F}_{3^n}$, где $n \geqslant 2$, существует такой ненулевой квадрат u, что $u + 1$ — тоже ненулевой квадрат.*

Доказательство. Если 2 — квадрат, то $u = 1$ — искомый элемент. Иначе предположим, что для любого $u \notin \{0, 1, 2\}$ верно следующее утверждение: если u — квадрат, то $u + 1$ — не квадрат. Тогда в любом множестве вида $\{u, u + 1, u + 2\}$ не более одного квадрата. Значит, всего квадратов не больше $3^{n-1} + 1$. С другой стороны, в поле характеристики 3 квадратов ровно $(3^n + 1)/2$. Отсюда получаем неравенство $(3^n + 1)/2 \leqslant 3^{n-1} + 1$, которое выполняется только при $n = 1$. Лемма доказана. $\square$

Вернёмся к доказательству теоремы 3. Итак, мы хотим показать, что в конечном поле характеристики три и порядка по крайней мере девять каждый элемент имеет уравновешенное нестепенное разложение в произведение трёх множителей.

Отметим, что в таком поле любой элемент является кубом ровно одного элемента. Будем искать сбалансированное разложение элемента $a = 2b^3 \neq 0$: $a = xyz$, $x + y + z = 0$. Избавляясь от z, получаем
$$yx^2 + y^2x + a = 0. \tag{$*$}$$
Будем решать это уравнение относительно x. По лемме существует такой $\tau^2 \neq 0$, что $\tau^2 + 1 = \pi^2 \neq 0$ тоже квадрат. Возьмём $y = b + b\pi$. Значит, дискриминант квадратного уравнения $(*)$ является квадратом:
$$\begin{aligned} D = y^4 - 4ay = y(y^3 - 8b^3) = y(y - 2b)^3 = (b\pi + b) \cdot (b\pi - b)^3 = \\ = b^2(\pi^2 - 1)(b\pi - b)^2 = b^2\tau^2(b\pi - b)^2 \end{aligned}$$

и у уравнения $(*)$ есть решение. Полученное разложение не будет степенным, так как $y^3 \neq a$. Действительно, иначе $2b^3 = b^3(1+\pi)^3 = b^3(1+\pi^3)$, откуда $\pi^3 = 1$, $\pi = 1$ и $\tau = 0$, что неверно.

Осталось найти нестепенное уравновешенное разложение нуля, но это легко: $0 = (-1) \cdot 1 \cdot 0$.

Случай 7: $|F| = 2^n$ и $k = 4 + 2m$, где $m \geqslant 0$, $n > 1$. Так как $\operatorname{char} F = 2$, любой элемент поля является квадратом: $a = b \cdot b$. Если $a \neq 1$, то $b \neq 1$ и $a = b^2 \cdot 1^{2m+2}$ — искомое разложение. Если $a = 1$, то $a = 1 = c^2 \cdot (1/c)^2 \cdot 1^{2m}$ — искомое разложение, где c — любой элемент, отличный от нуля и единицы.

Случай 8: $|F| = 3$ и $k = 3$ — нет. В разложении единицы не может участвовать нуль, а 1 и -1 обязаны участвовать, чтобы разложение было нестепенным. Тогда третий множитель — нуль, так как разложение уравновешенное. Это противоречие завершает доказательство теоремы 3. $\square$

§ 2. Матрицы

Доказательство теоремы 2. Сперва заметим, что при $k = 2$ теорема верна по простой причине:

> жорданова клетка J размера $n \times n$ с собственным значением нуль не является квадратом в кольце матриц $n \times n$ при $n \geqslant 2$

(доказательство этого утверждения мы оставляем читателям в качестве простого упражнения) и, следовательно, матрица $-J$ не обладает сбалансированным разложением в произведение двух сомножителей.

В случае $k \geqslant 3$ по теореме 3 нам достаточно доказать следующее утверждение.

Теорема 2$'$. *Пусть $n \geqslant 2$ и $k \geqslant 3$ — целые числа и F — поле (необязательно конечное). Тогда следующие условия равносильны*:

а) *каждая матрица $n \times n$ над F обладает уравновешенным разложением в произведение k коммутирующих множителей*;

б) *каждый элемент поля F обладает нестепенным уравновешенным разложением в произведение k множителей.*

Доказательство. Импликация б) $\Rightarrow$ а) сразу вытекает из следующего факта, доказанного в [4].

> Пусть F — поле и k — натуральное число, большее двух. Если во всех конечных расширениях поля F каждый элемент обладает нестепенным сбалансированным разложением в произведение k элементов, то это же верно для каждого элемента каждой конечномерной ассоциативной алгебры с единицей над F.

Импликация а) $\Rightarrow$ б). Заметим, что $0 \in F$ имеет нестепенное уравновешенное разложение в произведение k множителей для любого $k \geqslant 3$: $0 = 0^{k-2} \cdot 1 \cdot (-1)$. Чтобы разложить ненулевой элемент $a \in F$, нам понадобится следующий простой факт из линейной алгебры, доказательство которого мы тоже оставляем читателям в качестве упражнения:

> централизатор нильпотентной жордановой клетки J размера $n \times n$ в алгебре матриц $n \times n$ состоит из многочленов от J, т. е. $C(J) = \{a_0E + a_1J + \ldots + a_{n-1}J^{n-1} \mid a_i \in F\}$.

Теперь если жорданова клетка $aE + J$ обладает сбалансированным разложением $aE + J = X_1 \ldots X_k$ в произведение коммутирующих матриц, то все эти матрицы X_i лежат в централизаторе матрицы J и, в силу упомянутого выше факта, мы получаем уравновешенное разложение элемента a в поле F: $a = x_1 \ldots x_k$, где x_i — единственное собственное значение матрицы X_i. Остаётся заметить, что это разложение не может быть степенным при $a \neq 0$. Действительно, предположив противное, мы бы получили такое уравновешенное разложение в кольце матриц: $aE + J = (xE + J_1) \ldots (xE + J_k)$, где J_i — некоторые нильпотентные коммутирующие матрицы. Уравновешенность этого разложения означает, что k делится на $\operatorname{char} F$ и $\sum J_i = 0$. Но тогда, раскрывая скобки, мы получаем

$$aE + J = (xE + J_1) \ldots (xE + J_k) = aE + f(J_1, \ldots, J_k),$$

где многочлен f не имеет членов первой степени, т. е. в правой части равенства стоит матрица $aE + J'$, где $(J')^{n-1} = 0$ и, значит, $J' \neq J$. Полученное противоречие завершает доказательство теорем $2'$ и 2. $\square$

Без условий коммутативности вопрос об уравновешенных разложениях в алгебрах матриц над конечными полями остаётся открытым.

Вопрос. При каких q, k и n верно, что всякая матрица размера $n \times n$ над полем из q элементов имеет уравновешенное разложение в произведение k матриц того же размера?

Мы можем сказать лишь следующее.

1. В некоторых случаях разложение существует по теореме 2.

2. При $k = 2 \leqslant n$ разложения нет по теореме 2 (поскольку сомножители такого уравновешенного разложения обязательно коммутируют).

Кроме того, компьютерные эксперименты показывают следующее.

3. Над полем из двух элементов все матрицы 2×2, кроме $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ и (подобной ей матрицы) $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, допускают уравновешенное разложение в произведение трёх сомножителей, а эти две матрицы не имеют таких разложений.

4. Матрица $\begin{pmatrix}1&0\\1&1\end{pmatrix}$ и две подобные ей матрицы над полем из двух элементов не имеют уравновешенных разложений в произведение четырёх множителей, а остальные матрицы 2×2 над $\mathbb{F}_2$ имеют такие разложения.

5. Матрица $\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix}$ и подобные ей матрицы над полем из двух элементов не имеют уравновешенных разложений в произведение трёх множителей, а остальные матрицы 3×3 над $\mathbb{F}_2$ имеют такие разложения.

6. Все матрицы 3×3 над $\mathbb{F}_2$ имеют уравновешенные разложения в произведение четырёх множителей.

7. Все матрицы 2×2 над полями $\mathbb{F}_3$, $\mathbb{F}_4$, $\mathbb{F}_5$ и $\mathbb{F}_7$ имеют уравновешенные разложения в произведение трёх и четырёх множителей. Отсюда вытекает, что и для любого большего числа множителей это верно, поскольку мы можем увеличивать количество множителей на два, умножая имеющееся разложение на E и $-E$.

Список литературы

[1] *Васильев А. Н.* Казахстанская республиканская олимпиада по математике. 2013. Заключительный этап. 9 класс. Задача 4. http://matol.kz/olympiads/151

[2] *Васильев А. Н.* Девятая студенческая олимпиада по алгебре в МГУ. 2014. Задача 3. http://halgebra.math.msu.su/Olympiad/

[3] *Иванищук А. В.* Из опыта учебно-исследовательской деятельности учащихся в лицее 1511 при МИФИ // *Сгибнев А. И.* Исследовательские задачи для начинающих. М.: МЦНМО, 2015. С. 21–25. http://www.mccme.ru/free-books/sgibnev-issl.pdf

[4] *Klyachko A. A., Vassiliyev A. N.* Balanced factorizations // American Mathematical Monthly. 2016. V. 123, № 10. P. 989–1000. См. также https://arxiv.org/abs/1506.01571

Антон Александрович Клячко, мехмат МГУ
klyachko@mech.math.msu.su

Андрей Михайлович Мажуга, мехмат МГУ
mazhuga.andrew@yandex.ru

Анастасия Николаевна Понфиленко, мехмат МГУ
stponfilenko@gmail.com