УДК 512.772.7 + 512.624.3 + 512.552 MSC: 12E12, 14H52, 16U99, 16P10

# УРАВНОВЕШЕННЫЕ РАЗЛОЖЕНИЯ НА МНОЖИТЕЛИ

Антон Н. Васильев[♭] Антон А. Клячко[♯]

[♭] *Казахстанский филиал Московского государственного университета*
*Астана 010010, ул. Кажимукана 11, МГУ*
*antonvassilyev@mail.ru*
[♯] *Механико-математический факультет Московского государственного университета*
*Москва 119991, Ленинские горы, МГУ*
*klyachko@mech.math.msu.su*

*Всякое рациональное число можно разложить в произведение нескольких рациональных чисел, сумма которых равна нулю.* Это простое, но нетривиальное, утверждение предлагалось в качестве задачи на олимпиаде для школьников. Мы полностью решаем аналогичные вопросы в конечных полях и в некоторых других кольцах, например, в алгебрах комплексных и вещественных матриц, а также формулируем несколько открытых вопросов.

## 0. Введение

Задача, упомянутая в аннотации, была придумана первым автором и предлагалась на Казахстанской республиканской математической олимпиаде для школьников в 2013 году [Вас13]. Аналогичный вопрос для произвольного поля характеристики не два предлагался на студенческой олимпиаде по алгебре в МГУ в 2014 году [Вас14]. Позже нам стало известно, что задача рассматривалась и раньше [Ива13] (также в контексте работы со способными школьниками).

Вопрос о наличии таких уравновешенных разложений на множители решается легко в любом поле характеристики не два (смотрите теорему 0 ниже). Гораздо труднее выяснить сколько множителей могут содержать такие разложения. Этот вопрос уже сильно выходит за рамки олимпиад и является основным предметом изучения в этой статье. Например, в поле рациональных чисел пять множителей достаточно всегда, три — не всегда [Ива13], а всегда ли достаточно четырёх множителей — неизвестно.*)

В первом параграфе мы доказываем несколько общих фактов об уравновешенных разложениях и полностью решаем вопрос о возможном количестве сомножителей во всех конечных полях. Ответ получается неожиданным и довольно сложным (теорема 1). Например, оказывается, что во всех конечных полях, кроме ровно одного, каждый элемент допускает уравновешенное разложение в произведение не более чем трёх множителей. В роли единственного исключения выступает семиэлементное поле $\mathbb{F}_7$. Основным инструментом при работе в конечных полях нам служит оценка Хассе числа рациональных точек эллиптической кривой над конечным полем.

Кроме того, в первом параграфе мы показываем, что в каждом поле характеристики не 2 есть «универсальные» формулы, позволяющие получить уравновешенное разложение почти любого элемента. Например, формула (1) даёт уравновешенное разложение на пять множителей для любого ненулевого элемента (в любом поле характеристики не два). Мы доказываем, что такие формулы существуют для разложение на любое число сомножителей, начиная с пяти, но не существуют для разложение на три сомножителя. Этот факт мы выводим из теоремы Мейсона–Стотерса (то есть из $abc$-теоремы для многочленов).

Во втором параграфе мы показываем, что вопрос об уравновешенных разложениях в конечномерных алгебрах по существу сводится к аналогичному вопросу о полях и полностью решаем вопрос о количестве множителей в некоторых естественных алгебрах, например, в матричных алгебрах над $\mathbb{C}$ и $\mathbb{R}$.

В третьем параграфе мы приводим много примеров, показывающих, что результаты параграфа 2 не могут быть усилены в разных направлениях.

Последний параграф посвящён открытым вопросам.

Мы завершаем это краткое введение формальным определением нашего предмета изучения. Пусть некоторый элемент $a$ некоторого кольца некоторым образом разложен на множители в этом кольце: $a = a_1 a_2 \dots a_k$. Мы называем это разложение *уравновешенным* или *сбалансированным*, если $\sum a_i = 0$.

Авторы благодарят Ю. Г. Прохорова и М. А. Цфасмана, а также (студенток) Евгению Кошелеву, Алису Пикулину, Надиру Шокетаеву и (школьника) Рауана Жакыпбека за полезные обсуждения. Мы благодарны также анонимным рецензентам за ценные замечания.

Работа первого автора выполнена при поддержке Комитета науки Министерства образования и науки Республики Казахстан, грант ГФ4-0816.

Работа второго автора выполнена при поддержке Российского фонда фундаментальных исследований, грант №15-01-05823.

*) Когда эта работа была написана, мы поняли, что достаточно [KMP16].

## 1. Поля

**Теорема 0.** *В поле характеристики, отличной от двух, каждый элемент раскладывается в произведение $k$ сомножителей, сумма которых равна нулю, для каждого $k \geqslant 5$. А для каждого $k < 5$ найдётся поле характеристики не два, в котором аналогичное утверждение неверно.*

**Доказательство.** Докажем первое утверждение. Для нулевого элемента доказывать нечего, а для ненулевого элемента $a$ мы можем торжественно написать

$$a = \frac{a}{2} \cdot \frac{a}{2} \cdot (-a) \cdot \frac{2}{a} \cdot \left(-\frac{2}{a}\right). \tag{1}$$

Это даёт сбалансированное разложение на пять сомножителей. Лёгкая модификация разложения (1) даёт сбалансированное разложение произвольного элемента $b$ на шесть сомножителей:

$$b = c^2 - ca = \frac{a}{2} \cdot \frac{a}{2} \cdot (c-a) \cdot \frac{2}{a} \cdot \left(-\frac{2}{a}\right) \cdot (-c), \quad \text{где } c \text{ — любой элемент такой, что } 0 \neq c^2 \neq b, \text{ а } a = \tfrac{c^2-b}{c}.$$

(Такое $c$ обязательно найдётся, кроме случая, когда поле состоит из трёх элементов и $b = 1$; а в этом исключительном случае можно взять очевидное разложение $b = 1 = 1^3(-1)^3$.)

Сбалансированные разложения на $k \geqslant 7$ сомножителей можно получать, умножая полученные разложения на сбалансированные разложений минус единицы на два сомножителя: $-1 = (-1) \cdot 1$. Например, мы получаем такое сбалансированное разложение произвольного элемента в произведение ста сомножителей:

$$-b = -(c^2 - ca) = \frac{a}{2} \cdot \frac{a}{2} \cdot (c-a) \cdot \frac{2}{a} \cdot \left(-\frac{2}{a}\right) \cdot (-c) \cdot (-1)^{47} \cdot 1^{47}.$$

Первое утверждение доказано.

Второе утверждение вытекает из теоремы 1 (см. ниже): если $k \leqslant 3$, то в качестве примера годится поле $\mathbb{F}_7$, а если $k = 4$, то годится $\mathbb{F}_3$. Теорема доказана.

**Теорема 1.** *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*

*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 $k \neq 2$.*

Другими словами, ситуация в конечных полях такая:

| | $k=2$ | $k=3$ | $k=4$ | $k=5,7,9,\ldots$ | $k=6,8,10,\ldots$ |
|---|---|---|---|---|---|
| $\mathbb{F}_2$ | 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 |

**Доказательство.** Будем доказывать по столбцам этой таблицы.

**Случай $k = 2$.** В конечном поле характеристики два всякий элемент является квадратом (поскольку порядок мультипликативной группы такого поля нечётный), то есть каждый элемент является произведением двух одинаковых сомножителей, сумма которых равна нулю, поскольку характеристика равна двум. Если же характеристика конечного поля не равна двум, то не каждый элемент является квадратом и, следовательно, не каждый элемент раскладывается в произведение двух сомножителей, сумма которых равна нулю.

**Случай $k = 3$.** Если характеристика равна трём, то порядок мультипликативной группы поля $q - 1 = 3^k - 1$ не делится на три и, следовательно, каждый элемент является кубом и разложение $a = bbb$ является искомым (поскольку $b + b + b = 0$ в поле характеристики три).

Для доказательства в случае другой характеристики нам понадобится известная оценка Хассе (или Хассе–Вейля).

**Оценка Хассе** (см., например, [Sil86], теорема V.1.1)**.** *Число точек эллиптической кривой (то есть неособой и неприводимой над замыканием поля проективной кривой рода один) над конечным полем из $q$ элементов не меньше чем $q+1-2\sqrt{q}$.*
*В частности, это верно для неособых и неприводимых (над замыканием поля) кубических кривых в проективной плоскости над $\mathbb{F}_q$.*

Продолжим доказательство, считая, что характеристика поля отлична от трёх. Мы хотим показать, что система уравнений

$$\begin{cases} x+y+z=0 \\ xyz=a \end{cases} \tag{2}$$

над конечным полем $\mathbb{F}_q$ имеет по крайней мере одно решение для любого $a \in \mathbb{F}_q$. Другими словами, мы хотим показать, что кубическая (аффинная) кривая, заданная уравнением

$$xy(x+y) = -a,$$

имеет по крайней мере одну точку над $\mathbb{F}_q$. В однородных координатах соответствующая проективная кривая задаётся уравнением

$$XY(X+Y) = -aZ^3, \tag{3}$$

а особые точки этой кривой задаются системой уравнений, состоящей из уравнения (3) и его частных производных по $X$, $Y$ и $Z$:

$$\begin{cases} XY(X+Y) = -aZ^3 \\ 2XY + Y^2 = 0 \\ 2XY + X^2 = 0 \\ -3aZ^2 = 0 \end{cases}. \tag{4}$$

Мы считаем, что $a \neq 0$, поскольку при $a=0$ система (2) очевидно имеет решение (нулевое). Поэтому (и поскольку характеристика поля отлична от трёх) из последнего уравнения системы (4) мы получаем $Z=0$. Разность второго и третьего уравнения показывает, что $X = \pm Y$ и тогда второе уравнение показывает, что $X$ и $Y$ нулевые (мы опять воспользовались тем, что $\operatorname{char}\mathbb{F}_q \neq 3$). Таким образом, система (4) не имеет ненулевых решений, то есть наша проективная кривая не имеет особых точек над замыканием поля (если $\operatorname{char}\mathbb{F}_q \neq 3$). Это автоматически означает, что наша кривая неприводима (и, следовательно, эллиптична), поскольку приводимая кубическая кривая обязательно имеет особые точки (над замыканием поля)— это точки пересечения компонент.

Таким образом, мы можем применить оценку Хассе и получить, что проективная кубика (3) имеет больше трёх точек над полем $\mathbb{F}_q$, если характеристика этого поля не равна трём и $q+1 > 2\sqrt{q}+3$. Это неравенство выполнено при $q \geqslant 8$. Таким образом, при $q \geqslant 8$ проективная кривая содержит больше трёх точек, что означает, что соответствующая аффинная кривая содержит по крайней мере одну точку, поскольку пересечение неприводимой кубики с бесконечно удалённой прямой не может содержать больше трёх точек*), то есть система (2) имеет решение, что и требовалось.

Осталось разобраться с полями $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_5$ и $\mathbb{F}_7$.

В $\mathbb{F}_2$ единица очевидно не имеет сбалансированных разложений в произведение трёх сомножителей.

В $\mathbb{F}_4$ ненулевое сбалансированное произведение $xyz$ трёх сомножителей не может содержать повторяющихся множителей (поскольку $x+x=0$), поэтому такое произведение всего одно — это произведение всех ненулевых элементов поля, оно равно единице; следовательно, элементы, отличные от единицы и нуля, не допускают сбалансированных разложений в произведение трёх сомножителей.

В $\mathbb{F}_5$ система (2) имеет решение: $x=y=b$, $z=-2b$, где $b$ — кубический корень из $-\frac{a}{2}$ (в $\mathbb{F}_5$ любой элемент является кубом).

Поле из семи элементов действительно является исключением. В самом деле, элементы $\pm 3$ не имеют сбалансированных разложений в произведение трёх сомножителей. Действительно, если

$$\begin{cases} x+y+z=0 \\ xyz=\pm 3 \end{cases},$$

то элементы $x$, $y$ и $z$ обязаны быть попарно разными, поскольку $\pm 3$ не является удвоенным кубом (кубами в $\mathbb{F}_7$ являются элементы 0 и $\pm 1$). Разумеется, никакие два из элементов $x$, $y$ и $z$ не могут отличаться знаком. Остаётся только одна возможность (с точностью до знаков и перестановок): $x=\pm 1$, $y=\pm 2$, и $z=\pm 3$. Но произведение таких трёх чисел даёт $\pm 1$, а не $\pm 3$. (Тройка имеет, правда, более короткое сбалансированное разложение: $3 = 2\cdot(-2)$, но элемент $-3$ не имеет таких разложений.)

*) В нашем случае бесконечно удалённых точек на кривой ровно три: $(1,0,0)$, $(0,1,0)$ и $(1,-1,0)$ (в однородных координатах).

**Случай $k = 4$.** Будем искать сбалансированное разложение элемента $a \in F$ в произведение четырёх сомножителей, один из которых равен единице. Дальнейшие рассуждения (до некоторого момента) аналогичны доказательству при $k = 3$. Мы хотим показать, что система уравнений

$$\begin{cases} x + y + z + 1 = 0 \\ xyz = a \end{cases} \tag{2'}$$

над конечным полем $\mathbb{F}_q$ имеет по крайней мере одно решение для любого $a \in \mathbb{F}_q$. Другими словами, мы хотим показать, что кубическая (аффинная) кривая, заданная уравнением

$$xy(x + y + 1) = -a,$$

имеет по крайней мере одну точку над $\mathbb{F}_q$. В однородных координатах соответствующая проективная кривая задаётся уравнением

$$XY(X + Y + Z) = -aZ^3, \tag{3'}$$

а особые точки этой кривой задаются системой уравнений, состоящей из уравнения (3′) и его частных производных по $X$, $Y$ и $Z$:

$$\begin{cases} XY(X + Y + Z) = -aZ^3 \\ 2XY + Y^2 + YZ = 0 \\ 2XY + X^2 + XZ = 0 \\ XY = -3aZ^2 \end{cases}. \tag{4'}$$

Разность второго и третьего уравнения есть $Y^2 - X^2 + Z(Y - X) = 0$. Таким образом, либо $X + Y + Z = 0$, либо $X = Y$.

Если $X+Y+Z = 0$, то из первого уравнения (4′) получаем $Z = 0$. Из последнего уравнения тогда получаем, что $XY = 0$, и, следовательно все неизвестные равны нулю (поскольку мы предположили, что $X + Y + Z = 0$).

Если же $X = Y$, то второе уравнение системы (4′) показывает, что $3X^2 + XZ = 0$. Если здесь $X = 0$, то и $Y = 0$ и, следовательно, $Z = 0$ (из первого уравнения системы (4′)). Значит, $X \neq 0$ и сокращая на $X$ мы получаем $3X + Z = 0$. Тогда из последнего уравнения системы (4′) мы получаем $27a = -1$. Таким образом, если $27a \neq -1$ и $|F| \geqslant 8$, то мы можем воспользоваться оценкой Хассе и заключить, что $a \in F$ имеет сбалансированное разложение в произведение четырёх сомножителей (один из которых равен единице), Если же $27a = -1$, то мы действительно получаем особую точку на кривой, но сама эта особая точка, не будучи бесконечно удалённой, даёт сбалансированное разложение элемента $a$:

$$-\frac{1}{27} = \left(-\frac{1}{3}\right) \cdot \left(-\frac{1}{3}\right) \cdot \left(-\frac{1}{3}\right) \cdot 1.$$

Осталось рассмотреть маленькие поля $F$, где $|F| < 8$. В $\mathbb{F}_2$ и в $\mathbb{F}_4$ (как и в любом конечном поле характеристики два) любой элемент является четвёртой степенью некоторого другого элемента, что и даёт сбалансированное разложение в произведение четырёх (одинаковых) сомножителей.

В $\mathbb{F}_3$ единственное ненулевое сбалансированное произведение четырёх сомножителей — это $1 \cdot 1 \cdot (-1) \cdot (-1)$ и оно равно единице, поэтому $-1$ не допускает таких разложений.

В $\mathbb{F}_5$ произведение четырёх ненулевых сомножителей может быть одного из следующих видов:

$$(\pm 1)\,(\pm 1)\,(\pm 1)\,(\pm 1)\,, \quad (\pm 1)\,(\pm 1)\,(\pm 1)\,(\pm 2)\,, \quad (\pm 1)\,(\pm 1)\,(\pm 2)\,(\pm 2)\,, \quad (\pm 1)\,(\pm 2)\,(\pm 2)\,(\pm 2)\,, \quad (\pm 2)\,(\pm 2)\,(\pm 2)\,(\pm 2)\,.$$

Первое, третье и пятое из этих произведений дают $\pm 1$, поскольку квадрат любого элемента равен $\pm 1$. А во втором и четвёртом произведении есть только по два способа расставить знаки так, чтобы сумма сомножителей оказалась нулевой:

$$1 \cdot 1 \cdot 1 \cdot 2, \quad (-1) \cdot (-1) \cdot (-1) \cdot (-2),$$
$$(-1) \cdot 2 \cdot 2 \cdot 2, \quad 1 \cdot (-2) \cdot (-2) \cdot (-2).$$

Все эти произведения равны двойке, поэтому $-2 \in \mathbb{F}_5$ не допускает сбалансированного разложения в произведение четырёх сомножителей.

В поле $\mathbb{F}_7$ подбираем уравновешенные разложения:

$$0 = 0^4, \quad 1 = 1^2 \cdot (-1)^2, \quad -1 = 1 \cdot 1 \cdot 2 \cdot 3, \quad 2 = 2^2 \cdot (-2)^2, \quad -2 = 1 \cdot (-2)^2 \cdot 3, \quad 3 = (-1) \cdot 2 \cdot 3^2, \quad -3 = (-1)^3 \cdot 3.$$

**Случай чётного $k > 4$.** Если каждый элемент $a$ имеет сбалансированное разложение в произведение $k$ сомножителей: $a = a_1 \dots a_k$, то каждый элемент имеет сбалансированное разложение в произведение $(k + 2)$-х сомножителей: $-a = a_1 \dots a_k \cdot 1 \cdot (-1)$. Поэтому достаточно доказать утверждение для $k = 6$. Более того,

для всех конечных полей, кроме $\mathbb{F}_3$ и $\mathbb{F}_5$, утверждение можно считать доказанным, поскольку у нас уже есть уравновешенное разложение каждого элемента в произведение четырёх сомножителей.

Для $\mathbb{F}_3$ имеем $0 = 0^6$, $\quad 1 = 1^6$, $\quad -1 = 1^3 \cdot (-1)^3$. А для $\mathbb{F}_5$ сбалансированное произведение $x \cdot x \cdot (-2x) \cdot 1 \cdot 1 \cdot (-2)$, равное $-x^3$, даёт произвольный элемент, поскольку все элементы являются кубами.

**Случай нечётного $k > 4$.** Такая же индукция, как в доказательстве при чётном большом $k$, позволяет свести дело к случаю $k = 5$. Более того, для всех конечных полей, кроме $\mathbb{F}_2$, $\mathbb{F}_4$ и $\mathbb{F}_7$, утверждение можно считать доказанным, поскольку у нас уже есть уравновешенное разложение каждого элемента в произведение трёх сомножителей.

В поле $\mathbb{F}_7$ искомое разложение существует по теореме 0. А в поле $\mathbb{F}_4$ мы можем написать $a = b^2xyz$, где $b$ — квадратный корень из $a$ и $x, y, z$ — все ненулевые элементы поля (их произведение равно единице, а сумма — нулю). В поле $\mathbb{F}_2$ уравновешенного разложения единицы в произведение нечётного числа сомножителей, очевидно, нет. Это завершает доказательство теоремы.

Формулу (1) можно рассматривать как «универсальную формулу», позволяющую сбалансировано разложить почти любой элемент поля характеристики не два в произведение пяти сомножителей (где *почти любой* означает любой, кроме конечного числа исключительных элементов). Теорема 0 показывает, что такие универсальные формулы существуют для каждого $k \geqslant 5$. Из доказательства теоремы 0 можно извлечь явный вид таких формул:

$$t = \underbrace{\frac{t}{2} \cdot \frac{t}{2} \cdot (-t) \cdot \frac{2}{t} \cdot \left(-\frac{2}{t}\right)}_{5 \text{ множителей}} = \underbrace{\frac{1-t}{2} \cdot \frac{1-t}{2} \cdot t \cdot \frac{2}{1-t} \cdot \frac{2}{t-1} \cdot (-1)}_{6 \text{ множителей}} = \underbrace{\left(-\frac{t}{2}\right) \cdot \left(-\frac{t}{2}\right) \cdot t \cdot \left(-\frac{2}{t}\right) \cdot \frac{2}{t} \cdot (-1) \cdot 1}_{7 \text{ множителей}} = \dots$$

Следующая теорема показывает, что «универсальной формулы» сбалансированного разложения на три сомножителя не существует (универсальных сбалансированных разложений на два множителя тоже, очевидно, не существует, а вопрос про четыре сомножителя остаётся открытым, смотрите последний параграф).

**Теорема об отсутствии формул.** *Элемент $t$ поля рациональных дробей $F(t)$ не допускает сбалансированного разложения на три множителя ни для какого поля $F$.*

**Доказательство.** Предположив противное, после приведения к общему знаменателю получаем тождество

$$t^s = \frac{x(t)}{v(t)} \cdot \frac{y(t)}{v(t)} \cdot \frac{z(t)}{v(t)}, \quad \text{где } x, y, z \in F[t] \text{ и } x + y + z = 0.$$

Мы хотим показать, что $s$ не может быть единицей, но удобно доказывать более общий факт:

*написанные выше равенства влекут, что $s$ делится на три.*

Ясно, что многочлены $x$, $y$ и $z$ можно считать взаимно простыми, поскольку равенство $xyz = t^s v^3$ показывает, что их общий неприводимый делитель обязан делить $v$ или совпадать с $t$; в обоих случаях всё можно сократить. Кроме того, можно считать, что $v(0) \neq 0$ (увеличивая $s$, если нужно).

Воспользуемся известной теоремой Мейсона–Стотерса ([May84], [Sto81]), изложенной во многих книгах (см., например, [Lang02]). Мы предпочитаем пользоваться версией Снайдера, которая работает в любой характеристике.

**Теорема Мейсона–Стотерса** (в форме Снайдера [Sny00])**.** *Если три многочлена $x, y, z \in F[t]$ над произвольным полем $F$ взаимно просты и $x + y + z = 0$, то либо степень каждого из них строго меньше числа различных корней произведения $xyz$ в алгебраическом замыкании поля $F$, либо все три производные $x'$, $y'$ и $z'$ равны нулю (как многочлены).*

В нашей ситуации $xyz = t^s v^3$ и число различных корней этого многочлена не превосходит $\deg v + 1$, поэтому по теореме Мейсона–Стотерса либо степень каждого из многочленов $x, y, z$ не превосходит степени многочлена $v$, либо $x' = y' = z' = 0$.

В первом случае $\deg(xyz) \leqslant 3 \deg v$, что означает, что $s = 0$ (поскольку $xyz = t^s v^3$) и всё доказано. А во втором случае производная произведения равна нулю: $0 = (xyz)' = (t^s v^3)' = st^{s-1}v^3 + 3t^s v^2 v' = v^2 t^{s-1}(sv + 3tv')$, сокращая на $v^2 t^{s-1}$, мы получаем $sv = -3tv'$. Это означает, что $s$ делится на $\operatorname{char} F$, поскольку $v(0) \neq 0$. Значит, либо $\operatorname{char} F = 3$ и $s$ делится на три, что и требовалось, либо $v' = 0$.

Если $v' = 0$, то вспомним, что равенство $f' = 0$ означает, что многочлен $f$ представляет собой многочлен вида

$$f(x) = f_1(x^p), \quad \text{где } p \text{ — это характеристика поля, а } f_1 \text{ — это какой-то многочлен.}$$

Значит подставляя в равенство, с которого мы начали,

$$x(t) = x_1(t^p), \quad y(t) = y_1(t^p), \quad z(t) = z_1(t^p), \quad v(t) = v_1(t^p),$$

мы получаем, что $s$ делится на $p$ и, обозначая $t^p$ буквой $\tau$, мы получаем аналогичное равенство, но для многочленов меньшей степени (от $\tau$):

$$\tau^{\frac{s}{p}} = \frac{x_1(\tau)}{v_1(\tau)} \cdot \frac{y_1(\tau)}{v_1(\tau)} \cdot \frac{z_1(\tau)}{v_1(\tau)}, \quad \text{где } x_1, y_1, z_1 \in F[\tau] \text{ и } x_1 + y_1 + z_1 = 0.$$

Здесь степени всех многочленов уменьшились в $p$ раз. Очевидная индукция завершает доказательство.

## 2. Алгебры

**Лемма 1.** *Многочлен от одной переменной над ассоциативным коммутативным кольцом с единицей, у которого значение в некоторой точке $d$ нильпотентно, а значение производной в этой точке обратимо, обязательно имеет корень в этом кольце. При этом для некоторого корня $b$ разность $d - b$ делится на $f(d)$.*

**Доказательство.** Очевидная замена переменных сводит задачу к случаю, когда $d = 0$. Пусть наш многочлен над кольцом $R$ имеет вид $f(x) = a_0 + a_1x + \ldots + a_nx^n$ и нам известно, что $a_1$ обратим, $a_0^s = 0$. Будем доказывать индукцией по $s$, что *многочлен $f$ имеет корень, делящийся на $a_0$.*

В факторкольце $\overline{R} = R/(a_0^{s-1}R)$ образ $\overline{f}$ нашего многочлена $f$ имеет корень $\overline{ca_0}$ по предположению индукции. Возьмём какой-нибудь прообраз $c \in R$ элемента $\overline{c} \in \overline{R}$ и будем искать корень многочлена $f$ в виде $b = ca_0 + ta_0^{s-1}$, где $t \in R$ — (неизвестный) элемент. Поскольку $a_0^s = 0$, мы имеем

$$f(b) = a_0 + a_1(ca_0 + ta_0^{s-1}) + \ldots + a_n(ca_0 + ta_0^{s-1})^n = f(ca_0) + a_1ta_0^{s-1}. \tag{5}$$

Далее, поскольку $ca_0$ — корень многочлена $f$ по модулю идеала $a_0^{s-1}R$, мы имеем $f(ca_0) \in a_0^{s-1}R$, то есть $f(ca_0) = ra_0^{s-1}$ при некотором $r \in R$. Осталось заметить, что $f(b)$ в выражении (5) будет нулём, если мы возьмём $t = -r/a_1$, что и доказывает лемму.

Следующая теорема сводит вопрос о сбалансированных разложениях в конечномерных алгебрах к аналогичному вопросу о полях, если интересоваться только *нестепенными* разложениями, то есть такими разложениями, в которых не все сомножители равны между собой.

**Теорема 2.** *Пусть $F$ — поле и $n$ — натуральное число большее двух. Если во всех конечных расширениях поля $F$ каждый элемент обладает нестепенным сбалансированным разложением в произведение $n$ элементов, то то же верно для каждого элемента каждой конечномерной ассоциативной алгебры с единицей над $F$.*

**Доказательство.** Ясно, что утверждения достаточно доказать для конечномерных однопорождённых алгебр с единицей (поскольку любой элемент любой алгебры содержится в однопорождённой подалгебре). Таким образом, мы считаем, что наша алгебра $A$ над полем $F$ имеет вид $A = F[x]/(f)$, где $f \in F[x]$. Такая алгебра $A$ раскладывается, как известно, в прямую сумму

$$A \simeq \bigoplus_{i=1}^{m} F_i[x]/(x^{k_i}), \quad \text{где поля } F_i \text{ являются конечными расширениями поля } F$$

($F_i \simeq F[x]/(p_i)$, если $f = \prod p_i^{k_i}$ — разложение многочлена $f$ на неприводимые (над $F$) множители). Сбалансированные разложения достаточно получить для каждого прямого слагаемого по отдельности. Поэтому мы будем считать, что $A = G[x]/(x^k)$, где поле $G$ является конечным расширением поля $F$. Такая алгебра $A$ является локальной, то есть имеет единственный максимальный идеал $I$ (порождённый элементом $x$), $A/I \simeq G$ и все элементы, не лежащие в $I$, обратимы.

Мы хотим разложить произвольный элемент $a \in A$ в произведение $n$ элементов с нулевой суммой.
**Случай I.** $a \notin I$. В этом случае найдём нестепенное сбалансированное разложение элемента $a$ по модулю идеала $I$, то есть в поле $G$. Таким образом мы получим элементы $a_1, \ldots, a_n \in A$ такие, что

$$a - a_1a_2 \ldots a_n \in I, \quad a_1 + \ldots + a_n \in I \quad \text{и (без ограничения общности)} \quad a_1 - a_n \notin I.$$

Это означает, что для квадратного многочлена

$$g(t) = a + ta_2a_3 \ldots a_{n-1}(t + a_2 + a_3 + \ldots + a_{n-1}) \quad \text{мы имеем} \quad g(a_1) \in I. \tag{6}$$

Для производной многочлена $g$ мы получаем

$$g'(a_1) = a_2a_3\dots a_{n-1}(a_1 + a_2 + a_3 + \dots + a_{n-1}) + a_1a_2a_3\dots a_{n-1} \in a_2a_3\dots a_{n-1}(a_1 - a_n) + I.$$

Идеал $I$ состоит из нильпотентных элементов, а все не лежащие в нём элементы кольца $A$ обратимы. Поэтому условия леммы 1 выполнены, так как $a_1 \neq a_n \pmod I$. Применяя лемму 1, мы находим корень $\widetilde{t} \in A$ многочлена $g$, что и требовалось, поскольку

$$a = \widetilde{t}a_2a_3\dots a_{n-1}(-\widetilde{t} - a_2 - a_3 - \dots - a_{n-1}) \quad \text{и сумма множителей в этом разложении равна нулю.} \qquad (7)$$

Это разложение нестепенное, поскольку $\widetilde{t} = a_1 \pmod I$ по лемме 1, а $a_1 \neq a_n \pmod I$ по предположению.

**Случай II.** $a \in I$. Выберем обратимые (то есть не лежащие в $I$) элементы $a_2, \dots, a_{n-1} \in A$ так, чтобы их сумма тоже оказалась обратимой. Это очевидно возможно, если в поле $G = A/I$ больше двух элементов. Если же в поле $G$ два элемента, то единичный элемент этого поля не обладает в $G$ никаким нестепенным разложением, что противоречит условию.

Тогда для многочлена $g(t)$ (см. формулу (6)) мы имеем $g(0) = a$ — нильпотентный элемент и

$$g'(0) = a_2a_3\dots a_{n-1}(a_2 + a_3 + \dots + a_{n-1}) \text{ — обратимый элемент.}$$

Поэтому, по лемме 1 многочлен $g$ имеет корень $\widetilde{t} \in A$, что и требовалось (см. (7)). Разложение (7) не может быть степенным, поскольку элемент $a_2$ обратим, а элемент $a$ — нет.

Теорема доказана.

**Следствие 1.** *Каждый элемент конечномерной ассоциативной алгебры (над полем) с единицей раскладывается в произведение*

*а) трёх элементов, сумма которых равна нулю, если поле алгебраически замкнуто;*

*б) пяти элементов, сумма которых равна нулю, если характеристика поля не два.*

**Доказательство.** Первое утверждение немедленно вытекает из теоремы 2, поскольку в алгебраически замкнутом поле каждый элемент обладает нестепенным сбалансированным разложением в произведение трёх сомножителей (чтобы получить нестепенное сбалансированное разложение $a = a_1a_2a_3$ для данного элемента $a$, можно просто выбрать любой элемент $a_1$ такой, что $a_1^3 \neq a$, после чего $a_2$ и $a_3$ подобрать, воспользовавшись алгебраической (квадратичной) замкнутостью).

Чтобы доказать второе утверждение, достаточно сослаться на теоремы 2 и 0 и заметить, что формула (1) никогда не может представлять собой степенное разложение.

**Следствие 2.** *Для любого $k \geqslant 3$ всякую комплексную или вещественную матрицу можно разложить в произведение $k$ матриц над тем же полем, сумма которых равна нулю.*

**Доказательство.** Утверждение немедленно вытекает из теоремы 2, поскольку каждое вещественное или комплексное число $a$ допускает нестепенное сбалансированное разложение вида $a = x \cdot (x+1) \cdot 1^{k-3} \cdot (2 - k - 2x)$, поскольку это равенство представляет собой кубическое уравнение относительно $x$.

### 3. Алгебры. Примеры

В этом параграфе мы приведём примеры, показывающие, что никакие условия теоремы 2 и следствия 1 не могут быть отброшены.

**Пример 1.** Каждый элемент поля $\mathbb{F}_3$ из трёх элементов обладает сбалансированным разложением в произведение трёх сомножителей: $0 = 0\cdot0\cdot0$, $\quad 1 = 1\cdot1\cdot1$, $\quad 2 = 2\cdot2\cdot2$. Однако в двумерной алгебре $A = \mathbb{F}_3[x]/(x^2)$ над этим полем элемент $1 + x$ не допускает уравновешенных разложений в произведение трёх множителей, поскольку, как нетрудно заметить, разложение $1 = 1 \cdot 1 \cdot 1$ является единственным сбалансированным разложением единицы в поле $\mathbb{F}_3$; следовательно, разложение элемента $1 + x \in A$ обязано иметь вид $1 + x = (1 + kx)(1 + lx)(1 + mx)$ (где $k, l, m \in \mathbb{F}_3$), откуда получаем $k + l + m = 1$ и разложение не является сбалансированным. Этот пример показывает, что теорема 2 перестанет быть верной, если из неё исключить оговорку о том, что рассматриваются только нестепенные разложения.

**Пример 2.** В алгебре многочленов $F[x]$ над произвольным полем элемент $x$ вообще не обладает сбалансированными разложениями. Этот пример показывает, что условие конечномерности нельзя исключить из формулировки теоремы 2 и следствия 1.

**Пример 3.** В алгебре с нулевым умножением вообще никакой ненулевой элемент не обладает сбалансированными разложениями. Этот пример показывает, что условие наличия единицы нельзя исключить из формулировки теоремы 2 и следствия 1.

Что же касается условия $n > 2$, то его, в принципе, можно исключить из формулировки теоремы 2 по той причине, что оно очевидным образом вытекает из остальных условий: в поле всякое сбалансированное разложение нуля в произведение двух сомножителей обязано быть степенным. С другой стороны, в любом ненулевом кольце ноль обладает нестепенными разложениями в произведение трёх и любого большего числа сомножителей: $0 = 0^{2016} \cdot b \cdot (-b)$, где $b$ — ненулевой элемент. Однако есть следующий простой пример.

**Пример 4.** В поле комплексных чисел всякий ненулевой элемент обладает нестепенным сбалансированным разложением в произведение двух сомножителей, но нильпотентная жорданова клетка очевидно не обладает сбалансированным разложением в произведение двух сомножителей (ни над каким полем).

Пример 4 также показывает, что в следствии 2 нельзя исключить условие $k > 2$, а в следствии 1(а), нельзя заменить тройку на двойку. Следующий пример показывает, что в следствии 1(б) нельзя заменить пятёрку на меньшее число.

**Пример 5.** Как уже отмечалось (смотрите пример 1), в двумерной алгебре $A = \mathbb{F}_3[x]/(x^2)$ элемент $1 + x$ не допускает уравновешенного разложения на три сомножителя. В той же алгебре (как и просто в поле $\mathbb{F}_3$) минус единица не допускает, очевидно, уравновешенного разложения в произведение четырёх сомножителей, а единица не имеет уравновешенных разложений в произведение двух сомножителей.

**Пример 6.** В поле $\mathbb{F}_2$ единица, разумеется, не допускает сбалансированных разложений в произведение пяти сомножителей. Этот простой пример показывает, что условие на характеристику не может быть отброшено в следствии 1(б) (и в теореме 0).

### 4. Открытые вопросы

**Вопрос 1** (А. В. Иванищук [Ива13])**.** *Всякое ли рациональное число можно разложить в произведение четырёх рациональных чисел, сумма которых равна нулю?**)

**Вопрос 2.** *Во всяком ли поле каждый элемент можно разложить в произведение не более четырёх сомножителей, сумма которых равна нулю?*

**Вопрос 3.** *Существует ли универсальная формула уравновешенного разложения на четыре множителя? Более точно, допускает ли уравновешенное разложение на четыре множителя элемент $t$ поля рациональных дробей $\mathbb{C}(t)$ (или даже $\mathbb{Q}(t)$)?**)

**Вопрос 4.** *Что происходит в характеристике 2? Есть ли там универсальные формулы? Вообще, любой ли элемент любого поля допускает уравновешенное разложение?*

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ


[Bac13] Васильев А. Н. Казахстанская республиканская олимпиада по математике. 2013. Заключительный этап. 9 класс. Задача 4. `http://matol.kz/olympiads/151`

[Bac14] Васильев А. Н. Девятая студенческая олимпиада по алгебре в МГУ. 2014. Задача 3. `http://halgebra.math.msu.su/Olympiad/`

[Ива13] Иванищук А. В. Из опыта учебно-исследовательской деятельности учащихся в лицее 1511 при МИФИ // опубликовано в книге *Сгибнев А. И. Исследовательские задачи для начинающих. Москва: МЦНМО, 2013.* (Доступна здесь: `http://www.mccme.ru/free-books/`)

[KMP16] Klyachko A. A., Mazhuga A. M., Ponfilenko A. N. Balansed factorisations in some algebras. arXiv:1607.01957

[Lang02] Lang S. Algebra. New York, Berlin, Heidelberg: Springer-Verlag, 2002.

[Mas84] Mason R. C., Diophantine Equations over Function Fields, London Mathematical Society Lecture Note Series 96, Cambridge, England: Cambridge University Press, 1984.

[Sil86] Silverman J. H. The Arithmetic of Elliptic Curves. New York: Springer-Verlag, 1986.

[Sny00] Snyder N. An alternate proof of Mason's theorem. Elem. Math., 2000, 55:3, 93–94.

[Sto81] Stothers W. W., Polynomial identities and hauptmoduln, Quarterly J. Math., 1981, 32:3, 349–370.


*) Когда эта работа была написана, мы поняли, что ответы на на вопросы 1 и 3 положительны [KMP16].