

ПРЕПРИНТЫ ПОМИ РАН

ГЛАВНЫЙ РЕДАКТОР

С.В. Кисляков

РЕДКОЛЛЕГИЯ

**В.М.Бабич, Н.А.Вавилов, А.М.Вершик, М.А.Всемирнов, А.И.Генералов, И.А.Ибрагимов,
Л.Ю.Колотилина, Б.Б.Лурье, Ю.В.Матиясевич, Н.Ю.Нецветаев, С.И.Репин, Г.А.Серегин**

**Учредитель: Федеральное государственное бюджетное учреждение науки
Санкт-Петербургское отделение Математического института
им. В. А. Стеклова Российской академии наук**

**Свидетельство о регистрации средства массовой информации: ЭЛ №ФС 77-33560 от 16
октября 2008 г. Выдано Федеральной службой по надзору в сфере связи и массовых
коммуникаций**

Контактные данные: 191023, г. Санкт-Петербург, наб. реки Фонтанки, дом 27

телефоны: (812)312-40-58; (812) 571-57-54

e-mail: admin@pdmi.ras.ru

<http://www.pdmi.ras.ru/preprint/>

Заведующая информационно-издательским сектором Симонова В.Н

Мультипликативные моноиды \mathbb{F}_p -алгебр и абсолютные тензорные произведения конечных полей

Н. В. Дуров

Санкт-Петербургское отделение
Математического института
им. В. А. Стеклова РАН
ndourov@gmail.com

Июнь, 2012

ABSTRACT

Данная работа посвящена изучению следующего вопроса: может ли мультипликативный моноид нетривиальной (коммутативной) \mathbb{F}_p -алгебры быть изоморфен мультипликативному моноиду \mathbb{F}_ℓ -алгебры для различных простых p и ℓ ? Иначе говоря, определяется ли характеристика коммутативной алгебры над конечным полем ее мультипликативным моноидом?

Этот вопрос оказывается эквивалентен вопросу о разрешимости некоторого уравнения в сверхнатуральных числах, который обычно может быть отрицательно решен для конкретных p и ℓ .

Кроме того, данный вопрос оказывается эквивалентен тому, существует ли нетривиальное “абсолютное тензорное произведение” $\mathbb{F}_p \otimes \mathbb{F}_\ell$, при определенном понимании таких тензорных произведений — в смысле теории гиперколец или теории новых обобщенных колец.

Ключевые слова: мультипликативный моноид, конечное поле, гиперкольцо, обобщенное кольцо, абсолютное тензорное произведение, сверхнатуральные числа, поле из одного элемента

ПРЕПРИНТЫ
Санкт-Петербургского отделения
Математического института им. В. А. Стеклова
Российской академии наук

PREPRINTS
of the St. Petersburg Department of Steklov Institute of Mathematics

ГЛАВНЫЙ РЕДАКТОР
С. В. Кисляков

РЕДКОЛЛЕГИЯ
В. М. Бабич, Н. А. Вавилов, А. М. Вершик, М. А. Всемиров,
А. И. Генералов, И. А. Ибрагимов, А. А. Иванов, Л. Ю. Колотилина,
В. Н. Кублановская, Г. В. Кузьмина, П. П. Кулиш, Б. Б. Лурье,
Ю. В. Матиясевич, Н. Ю. Нецветаев, С. И. Репин, Г. А. Серегин,
В. Н. Судаков, О. М. Фоменко

1 Постановка задачи

Зафиксируем различные простые числа p и ℓ . Пусть A — нетривиальная \mathbb{F}_p -алгебра, B — нетривиальная \mathbb{F}_ℓ -алгебра. Обозначим через A^\times и B^\times мультипликативные моноиды этих алгебр, и пусть $\theta : A^\times \xrightarrow{\sim} B^\times$ — мультипликативный изоморфизм (т.е. изоморфизм мультипликативных моноидов алгебр A и B). Наша задача — выяснить, для каких пар (p, ℓ) такое возможно. Назовем ее “основной задачей”; если p и ℓ заданы, мы говорим об “основной задаче для (p, ℓ) ”.

В рамках данной работы все кольца и алгебры предполагаются ассоциативными, коммутативными, с единицей. Впрочем, для нашей основной задачи не так важно, рассматриваем ли мы только коммутативные алгебры A и B или нет.

1.1. (Случай некоммутативных A и B .) Докажем, что избавление от условия коммутативности алгебр A и B не влияет на разрешимость “основной задачи” для пары (p, ℓ) . В самом деле, если существуют нетривиальные некоммутативные \mathbb{F}_p -алгебра A' и \mathbb{F}_ℓ -алгебра B' вместе с мультипликативным изоморфизмом $\theta' : A'^\times \xrightarrow{\sim} B'^\times$, то достаточно рассмотреть центр A алгебры A' и центр B алгебры B' ; поскольку центр определяется полностью в терминах мультипликативного моноида, очевидно, что θ' индуцирует изоморфизм $\theta : A^\times \xrightarrow{\sim} B^\times$, и что A и B — нетривиальные коммутативные алгебры нужных характеристик.

1.2. (План доказательства.) Мы собираемся доказать, что “основная задача” для конкретной пары (p, ℓ) эквивалентна разрешимости некоторого уравнения в сверхнатуральных числах. Для этого мы последовательно применяем несколько редукций вида “если существуют мультипликативно изоморфные нетривиальные алгебры A и B характеристик p и ℓ , то можно предполагать, что они обладают определенными дополнительными свойствами”. Это достигается с помощью переформулировки нужных свойств и конструкций таким образом, чтобы они выражались исключительно в терминах мультипликативного моноида алгебры; тогда мультипликативный изоморфизм θ позволяет переносить такие конструкции с A на B . Последовательность наших редукций такова:

1.2.1. (Можно считать A и B коммутативными.) В самом деле, центр нетривиальной \mathbb{F}_p -алгебры нетривиален, и полностью определен (как подмножество) ее мультипликативным моноидом; см. **1.1**.

1.2.2. (Можно считать A и B целыми над простым подполем.) В самом деле, целые элементы x некоторой \mathbb{F}_p -алгебры A можно охарактеризовать, как “периодические относительно степеней”, т.е. такие, что $x^m = x^n$

для различных неотрицательных целых m и n . Тем самым мультипликативный изоморфизм θ обязан переводить целое замыкание \mathbb{F}_p в A в целое замыкание \mathbb{F}_ℓ в B ; заменив A и B на эти целые замыкания, мы можем считать A и B целыми над содержащимися в них простыми полями.

1.2.3. (Кроме того, можно считать A и B приведенными, т.е. без ненулевых нильпотентов.) Эта редукция — самая сложная в цепочке. Ясно, что θ переводит нильрадикал A в нильрадикал B ; однако нам придется научиться описывать фактор целой \mathbb{F}_p -алгебры по нильрадикалу в терминах ее мультипликативной структуры, что не так просто.

1.2.4. (Можно считать A и B алгебраическими расширениями своих простых подполей.) Здесь нам понадобится изучать идеалы, порожденные идемпотентами, и факторы по ним, и научиться описывать их только с помощью мультипликативной структуры алгебры. После этого мы выбираем с помощью леммы Цорна максимальный такой идеал, и переходим к факторалгебре по нему.

1.2.5. (Алгебраические расширения A конечного поля \mathbb{F}_p однозначно задаются степенью $\deg A$, понимаемой как сверхнатуральное число; мультипликативный моноид A^\times получается присоединением нуля к циклической группе порядка $p^{\deg A} - 1$.) Далее нам придется классифицировать алгебраические расширения конечных полей с помощью их степеней, и разобраться, как устроены их мультипликативные группы. Это и приведет нас к основному результату **6.7**: *“основная задача” разрешима для (p, ℓ) тогда и только тогда, когда уравнение $p^x - 1 = \ell^y - 1$ разрешимо в сверхнатуральных числах x и y* . Конечно, нам придется объяснить, что такое $a^x - 1$ для сверхнатурального x и натурального $a > 1$.

2 Целые и периодические элементы

Определение 2.1 (Периодические элементы моноида.) Пусть M — (мультипликативно записанный) коммутативный моноид, x — элемент M . Мы говорим, что x (m, n) -периодичен для целых $m \geq 0$, $n \geq 1$, если $x^{m+n} = x^m$. Мы говорим, что x периодичен, если он периодичен для какой-нибудь пары (m, n) . Мы говорим, что (m, n) есть модуль периодичности элемента x , если x (m, n) -периодичен, и если пара (m, n) лексикографически наименьшая среди всех пар с таким свойством.

2.1.1. (Подмоноид (m, n) -периодических элементов.) Очевидно, (m, n) -периодичные элементы образуют подмоноид $M_{m,n}$ в M , и эта конструкция устойчива относительно любого гомоморфизма моноидов: $f(M_{m,n}) \subset M'_{m,n}$ для любого гомоморфизма $f : M \rightarrow M'$.

2.1.2. (Подмоноид периодических элементов $M_{\text{per}} \subset M$.) Несложно видеть, что всякий (m, n) -периодичный элемент также (m', n') -периодичен для любого $m' \geq m$ и n' , делящегося на n . Отсюда следует, что произведение (m', n') -периодичного и (m'', n'') -периодичного элемента заведомо $(m' + m'', n'n'')$ -периодично, т.е. *периодические элементы образуют подмоноид $M_{\text{per}} \subset M$.*

2.1.3. (Моноиды, порожденные одним элементом.) Пусть M — моноид, $x \in M$ — произвольный его элемент. Обозначим через M_x подмоноид, порожденный x ; он состоит из всех степеней x . Очевидно, есть два подслучая:

- Все степени x различны. Тогда моноид M_x бесконечен, изоморфен \mathbb{N}_0 посредством $f : n \mapsto x^n$, а элемент x — непериодичен.
- Какие-то две степени x совпадают: $x^m = x^{m+n}$. Выберем такое равенство с наименьшим m , а среди всех таких — с наименьшим n . Тогда все элементы $1, x, x^2, \dots, x^{m+n-1}$ попарно различны: элемент x^k с $k < m$ не может равняться никакой другой степени согласно выбору m ; если же $x^{m+s} = x^{m+t}$ для некоторых $0 \leq s < t \leq m+n-1$, то $x^m = x^{m+s}x^{n-s} = x^{m+t}x^{n-s} = x^{m+(t-s)}$, что противоречит минимальности n . Отсюда немедленно следует, что (m, n) — модуль периодичности x , и что x (m', n') -периодичен если и только если $m' \geq m$ и n' делится на n .

Теорема 2.2 (Целые элементы над конечным кольцом.) Пусть A — коммутативное кольцо положительной характеристики m . Тогда периодические элементы (мультипликативного моноида) A — это в точности элементы кольца A , целые над его простым подкольцом $P = \mathbb{Z}/m\mathbb{Z}$.

Доказательство. Если элемент x периодичен, то он удовлетворяет уравнению целой зависимости $x^{m+n} - x^m = 0$ над простым подкольцом P . И наоборот, если x цел над P , то P -подалгебра $P[x] \subset A$ является конечно порожденным P -модулем, т.е. фактормодулем P^k для некоторого k . Отсюда следует, что $P[x] \subset A$ — конечное подкольцо, причем оно содержит все степени x ; поэтому все эти степени не могут быть попарно различны, т.е. x периодичен.

2.2.1. (Применение к основной задаче.) Мы уже видели в 1.2.2, что данная теорема позволяет нам свести “основную задачу” к случаю, когда коммутативные алгебры A и B целы над своими простыми подполями, поскольку целые замыкания простых подполей допускают описание в терминах мультипликативного моноида алгебры.

2.2.2. (Элементы, целые над “полем из одного элемента” \mathbb{F}_1 .) В каком-то смысле можно сказать, что периодические элементы — это элементы, целые над “полем из одного элемента” \mathbb{F}_1 . С этой точки зрения всякое конечное кольцо R — целое над \mathbb{F}_1 , и тогда **2.2** можно выразить так: “поскольку R — целое над \mathbb{F}_1 , целые R -алгебры обязаны быть одновременно и целыми \mathbb{F}_1 -алгебрами”. Мы видим, что обычное коммутативное кольцо “цело над \mathbb{F}_1 ”, если и только если его характеристика положительна, и оно цело над своим простым подкольцом (или, что равносильно, над \mathbb{Z}).

3 Приведенные и p -приведенные элементы

Определение 3.1 (Приведенные элементы моноида.) Пусть M — коммутативный моноид. Мы говорим, что элемент $x \in M$ приведен, если он $(1, m)$ -периодичен для некоторого $m \geq 1$, т.е. если $x^{m+1} = x$. Мы говорим, что x p -приведен для некоторого простого p , если он $(1, m)$ -периодичен для некоторого $m \geq 1$, взаимно простого с p .

3.1.1. (Альтернативное описание p -приведенности.) Поскольку для любого m , взаимно простого с p , существует некоторое k , для которого m делит $p^k - 1$, мы видим, что x p -приведен если и только если он $(1, p^k - 1)$ -периодичен для некоторого $k \geq 1$, т.е. если $x^{p^k} = x$. Обозначим через $F_p : M \rightarrow M$ “эндоморфизм Фробениуса” $x \mapsto x^p$, определенный на любом коммутативном моноиде M . Мы видим, что x p -приведен если и только если x является неподвижной точкой какой-нибудь степени Фробениуса: $F_p^k(x) = x$.

3.1.2. (Подмоноид приведенных элементов $M_{red} \subset M$.) Ясно, что произведение $(1, m)$ -периодического и $(1, m')$ -периодического элемента является $(1, mm')$ -периодическим, и потому приведенные элементы образуют подмоноид $M_{red} \subset M_{per} \subset M$, устойчивый относительно любых гомоморфизмов моноидов.

3.1.3. (Подмоноид p -приведенных элементов $M_{p-red} \subset M$.) Аналогично, p -приведенные элементы M образуют подмоноид M_{p-red} внутри M_{red} , устойчивый относительно любых гомоморфизмов моноидов.

Теорема 3.2 (p -приведенные элементы в \mathbb{F}_p -алгебре.) Пусть A — коммутативное кольцо, характеристика которого является степенью простого числа p . Пусть $\mathfrak{n}_A \subset A$ — нильрадикал, $A_{p-red} \subset A$ — подмоноид p -приведенных элементов. Тогда:

- а) Если A — \mathbb{F}_p -алгебра, то A_{p-red} — \mathbb{F}_p -подалгебра в A .

- b) Ограничение гомоморфизма $\pi : A \rightarrow A/\mathfrak{n}_A$ на подмоноид A_{p-red} индуцирует биекцию между A_{p-red} и целым замыканием \mathbb{F}_p в A/\mathfrak{n}_A .
- c) Если A — целая \mathbb{F}_p -алгебра, то A_{p-red} — приведенная \mathbb{F}_p -подалгебра в A , канонически изоморфная A/\mathfrak{n}_A .

Доказательство. а): В самом деле, если x и y p -приведены, то $F_p^k(x) = x$ и $F_p^{k'}(y) = y$ для некоторых $k, k' \geq 1$, откуда $F_p^{kk'}(x+y) = x+y$, так как в данном случае эндоморфизм Фробениуса является кольцевым эндоморфизмом A . Утверждение c), очевидно, следует из а) и б), так что осталось доказать б). Не умаляя общности, можно заменить A на целое замыкание простого подкольца в A , т.е. на A_{per} , и считать, что все элементы A периодичны (см. 2.2). Мы должны доказать, что ограничение проекции $\pi : A \rightarrow A/\mathfrak{n}_A$ на A_{p-red} биективно. Очевидно, достаточно доказать это для всевозможных конечно порожденных подалгебр $A' \subset A$, поскольку A является фильтрующимся индуктивным пределом всех таких A' , и аналогично $\mathfrak{n}_A = \varinjlim_{A'} \mathfrak{n}_{A'}$ и $A_{p-red} = \varinjlim_{A'} A'_{p-red}$. Поэтому мы можем считать, что алгебра A конечна.

Докажем, что ограничение π на A_{p-red} инъективно. Пусть $x, y \in A_{p-red}$ — два элемента A_{p-red} , сравнимых по модулю нильрадикала. Тогда $y = x + u$, $u^N = 0$, $x^{p^k} = x$ и $y^{p^k} = y$ для подходящих $k, N \geq 1$. Увеличив k , можно считать, что $u^{p^k} = 0$, и что $p^k \cdot 1 = 0$ в A ; тогда $y = y^{p^k} \equiv x^{p^k} + u^{p^k} = x^{p^k} = x \pmod{p}$. Далее, из $a \equiv b \pmod{p^s}$ следует $a^p \equiv b^p \pmod{p^{s+1}}$; применяя это k раз к x и y , мы получим $x = x^{p^k} \equiv y^{p^k} = y \pmod{p^{k+1}}$, откуда $x = y$, поскольку $p^k \cdot 1 = 0$ в A .

Осталось доказать, что любой элемент из A сравним по модулю нильрадикала с некоторым элементом из A_{p-red} . Для этого заметим, что факторкольцо A/\mathfrak{n}_A является конечной приведенной \mathbb{F}_p -алгеброй, и потому изоморфно произведению конечных полей $\mathbb{F}_{p^{k_1}} \times \cdots \times \mathbb{F}_{p^{k_s}}$. Пусть $k = k_1 \cdots k_s$; тогда k -ая степень Фробениуса действует тождественно на A/\mathfrak{n}_A , иначе говоря, $x^{p^k} = F_p^k(x) \equiv x \pmod{\mathfrak{n}_A}$ для любого $x \in A$. Возьмем теперь произвольный $x \in A$, и рассмотрим последовательность $x, x^{p^k}, x^{p^{2k}}, \dots$ элементов A ; поскольку A конечно, мы получим $x^{p^{mk}} = x^{p^{nk}}$ для некоторых $n > m \geq 0$. Очевидно, $x^{p^{mk}}$ является p -приведенным элементом, сравнимым с x по модулю нильрадикала.

3.2.1. (p -приведенные элементы как представители Тейхмюллера.) Естественно называть элементы из A_{p-red} *представителями Тейхмюллера* соответствующих элементов из A/\mathfrak{n}_A . Заметим, что они всегда образуют мультипликативный подмоноид в алгебре A , но подалгеброй он будет только в том случае, если A — \mathbb{F}_p -алгебра.

3.2.2. (Каноническая ретракция вложения $M_{p-red} \hookrightarrow M_{per}$.) Вложение $M_{p-red} \hookrightarrow M_{per}$ допускает каноническую ретракцию $\rho_p : M_{per} \rightarrow M_{p-red}$, определенную следующим образом. Пусть $x \in M_{per}$; тогда $x^{p^{m+n}} = x^{p^m}$ для некоторых $m \geq 0, n > 0$, поскольку моноид степеней x конечен. Положим $\rho_p(x) := x^{p^{n \lceil m/n \rceil}}$. Можно проверить, что $\rho_p(x)$ не зависит от выбора m и n , и что ρ_p — гомоморфизм моноидов, принимающий значения в M_{p-red} и тождественный на элементах из M_{p-red} .

3.2.3. (Случай $M = A^\times$: мультипликативное описание \equiv_{n_A} .) Пусть снова M — это мультипликативный моноид некоторой $\mathbb{Z}/p^k\mathbb{Z}$ -алгебры A . Тогда A_{per} совпадает с целым замыканием простого кольца в A , а A_{p-red} канонически изоморфен образу A_{per} при проекции $\pi : A \rightarrow A/\mathfrak{n}_A$ (см. 3.2). При этих отождествлениях ретракция $\rho_p : A_{per} \rightarrow A_{p-red}$ совпадает с ограничением π на A_{per} . В частности, если A — целая $\mathbb{Z}/p^k\mathbb{Z}$ -алгебра, то отношение эквивалентности \equiv_{n_A} допускает описание в терминах мультипликативной структуры A : $x \equiv_{n_A} y$ если и только если $\rho_p(x) = \rho_p(y)$.

3.2.4. (Каноническая ретракция вложения $M_{red} \hookrightarrow M_{per}$.) Вложение $M_{red} \hookrightarrow M_{per}$ также допускает каноническую ретракцию $\rho : M_{per} \rightarrow M_{red}$. Пусть $x \in M_{per}$; тогда $x^{m+n} = x^m$ для некоторых $m \geq 0, n > 0$, поскольку x периодичен. Положим $\rho(x) := x^{n \lceil m/n \rceil}$.

3.3. (Применение к основной задаче.) К сожалению, мы не можем сразу применить 3.2 к нашей основной задаче: конечно же, мультипликативный изоморфизм θ переводит подмоноид A_{p-red} в B_{p-red} , однако только A_{p-red} является подалгеброй A , изоморфной A/\mathfrak{n}_A , поскольку только A является \mathbb{F}_p -алгеброй. Представители Тейхмюллера для B/\mathfrak{n}_B образуют \mathbb{F}_ℓ -подалгебру $B_{\ell-red}$ внутри B , которая, однако, вовсе не обязана совпадать с B_{p-red} , поскольку $\ell \neq p$.

Нам придется пойти по более сложному пути: сначала проделать следующую редукцию и добиться, чтобы A и B были локальными целыми алгебрами над своими простыми подполями, а уже потом применять 3.2.

4 Идеалы, порожденные идемпотентами. Ортогональные суммы идемпотентов

Определение 4.1 (Моноид идемпотентов.) Пусть M — коммутативный моноид. Обозначим через $\text{Idem}(M) \subset M$ подмоноид, состоящий из идемпотентов $\{e \in M \mid e^2 = e\}$, т.е. $(1, 1)$ -периодических элементов. Будем рассматривать $\text{Idem}(M)$ как полурешетку относительно порядка $e \leq e' \Leftrightarrow ee' = e$; единица $1 \in \text{Idem}(M)$ является наибольшим элементом относи-

тельно этого порядка, а нижняя грань двух элементов $e \wedge e'$ совпадает с их произведением ee' .

4.1.1. (Делимость идемпотентов.) Заметим, что частичный порядок \leq на $\text{Idem}(M)$ может быть описан как отношение делимости в M или в $\text{Idem}(M)$: в самом деле, если $ee' = e$, то, очевидно, e делится на e' , и наоборот, если $e = xe'$, то $ee' = xe'e' = xe' = e$.

4.1.2. (Наименьший элемент и верхняя грань.) Если M — моноид с нулем, то 0 является наименьшим элементом $\text{Idem}(M)$. В некоторых случаях в $\text{Idem}(M)$ существует и верхняя грань $e \vee e'$ любых двух элементов e и e' . Например, это так, если $M = A^\times$ для некоторого кольца A : в этом случае $e \vee e' = e + e' - ee'$.

4.1.3. (Фактормоноид Me .) Пусть $e \in \text{Idem}(M)$. Тогда кратные $Me = \{xe : x \in M\}$ образуют подполугруппу в M , являющуюся моноидом с единицей e . Отображение $\varphi_e : x \mapsto xe$ является сюръективным гомоморфизмом моноидов $\varphi_e : M \rightarrow Me$; таким образом, Me может быть отождествлен с фактормоноидом M (но не с подмоноидом M). Очевидно, $\text{Idem}(Me)$ можно отождествить с подмножеством элементов $\text{Idem}(M)$, не превосходящих e .

Отметим, что $\varphi_e : M \rightarrow Me$ пропускается через $\varphi_{e'} : M \rightarrow Me'$, если и только если $e \leq e'$.

4.1.4. (Идемпотентные фактормоноиды.) Будем говорить, что N (или, вернее, $M \rightarrow N$) является *идемпотентным фактормоноидом*, если он изоморфен $M \rightarrow Me$ для некоторого идемпотента e . Несложно видеть, что e однозначно восстанавливается по $M \rightarrow N$ как наименьший идемпотент в M , отображающийся в единицу N .

Определение 4.2 (Ортогональные разложения.) Пусть e, e_1, \dots, e_n — идемпотенты из M . Мы говорим, что (e_i) представляют собой ортогональное разложение e , или что e есть ортогональная прямая сумма (e_i) , и пишем $e = e_1 \oplus e_2 \oplus \dots \oplus e_n$, если все $e_i \leq e$, и канонический гомоморфизм $Me \rightarrow Me_1 \times \dots \times Me_n$, $x \mapsto (xe_1, \dots, xe_n)$, является изоморфизмом.

4.2.1. (Ортогональная прямая сумма есть верхняя грань.) Заметим, что если $e = e_1 \oplus \dots \oplus e_n$, то $e = e_1 \vee \dots \vee e_n$; в частности, ортогональная прямая сумма однозначно определяется набором (e_i) . В самом деле, $e' \geq e$ если и только если e' отображается в единицу моноида Me при проекции $\varphi_e : M \rightarrow Me$; поскольку φ_e можно отождествить с отображением $(\varphi_{e_1}, \dots, \varphi_{e_n}) : M \rightarrow Me_1 \times \dots \times Me_n$, мы видим, что условие $e' \geq e$ равносильно условию $e' \geq e_i$ одновременно для всех i , откуда $e = e_1 \vee \dots \vee e_n$.

4.2.2. (Ортогональные прямые суммы дистрибутивны.) Если $e = e_1 \oplus \cdots \oplus e_n$, то $ee' = e_1e' \oplus \cdots \oplus e_ne'$ для любого идемпотента e' ; иначе говоря, $(e_1 \oplus \cdots \oplus e_n)e' = e_1e' \oplus \cdots \oplus e_ne'$. Чтобы увидеть это, рассмотрим изоморфизм моноидов $Me \cong Me_1 \times \cdots \times Me_n$; идемпотент ee' переходит при этом изоморфизме в идемпотент (e_1e', \dots, e_ne') . Теперь осталось рассмотреть фактормоноиды левой и правой части, определенные этими идемпотентами: получим $Me e' \cong Me_1e' \times \cdots \times Me_ne'$.

4.2.3. (Нули в ортогональных прямых суммах.) Заметим, что $e = e \oplus 0 \oplus 0 \cdots \oplus 0$ для любого количества нулей и любого идемпотента e в моноиде с нулем M . Наоборот, если $e = e_1 \oplus e_2 \oplus \cdots \oplus e_n$ и $e_1 = e$, то обязательно $e_2 = \cdots = e_n = 0$. В самом деле, отображение $Me \rightarrow Me \times Me_2 \times \cdots \times Me_n$, первая компонента которого — тождественное отображение, может быть изоморфизмом только если $Me_2 = \cdots = Me_n = 1$, т.е. если $e_2 = \cdots = e_n = 0$.

4.2.4. (Ассоциативность ортогональных прямых сумм.) Несложно видеть, что ортогональные прямые суммы коммутативны (не зависят от порядка аргументов) и ассоциативны в следующем смысле. Пусть I — конечное множество, $I = I_1 \sqcup \cdots \sqcup I_n$ — его разложение на n непересекающихся подмножеств, $(e_i)_{i \in I}$ — семейство идемпотентов, и предположим, что существуют все $E_j := \bigoplus_{i \in I_j} e_i$. Тогда $\bigoplus_{i \in I} e_i$ существует если и только если существует $\bigoplus_{1 \leq j \leq n} E_j$, и в этом случае оба эти идемпотента равны.

4.2.5. (Ортогональность зависит от всего M , а не только от $\text{Idem}(M)$.) Следует отметить, что отношение “ e есть ортогональная прямая сумма (e_i) ”, в отличие от отношения “ e есть верхняя грань (e_i) ” зависит от всего моноида M , а не только от подмоноида его идемпотентов $\text{Idem}(M)$.

Определение 4.3 (Связные моноиды и неприводимые идемпотенты.) Мы говорим, что моноид с нулем $M \neq 0$ связан, если в нем нет нетривиальных идемпотентов, т.е. если $\text{Idem}(M) = \{0, 1\}$. Мы говорим, что идемпотент $e \in \text{Idem}(M)$ неприводим, если моноид Me связан, или, что равносильно, если $e \neq 0$ и всякий идемпотент $0 \neq e' \leq e$ обязательно равен e .

Определение 4.4 (Ортогональные идемпотенты.) Пусть M — коммутативный моноид с нулем. Мы говорим, что идемпотенты e и e' ортогональны, если $ee' = 0$. Мы говорим, что семейство идемпотентов $(e_i)_{1 \leq i \leq n}$ ортогонально, если $e_i e_j = 0$ при $i \neq j$.

4.4.1. (Если существует ортогональная прямая сумма (e_i) , то (e_i) ортогонально.) Предположим, $e = e_1 \oplus \cdots \oplus e_n$ — ортогональная прямая

сумма в моноиде с нулем. Тогда семейство (e_i) ортогонально. В самом деле, согласно дистрибутивности **4.2.2**, $e_j = e_1e_j \oplus \cdots e_ne_j$; поскольку одно из слагаемых есть $e_je_j = e_j$, из **4.2.3** следует, что все $e_ie_j = 0$ при $i \neq j$.

Определение 4.5 (Устойчивые моноиды.) Мы будем говорить, что коммутативный моноид с нулем M устойчив, если в нем существуют ортогональные прямые суммы любых двух ортогональных идемпотентов: $e, e' \in \text{Idem}(M)$, $ee' = 0 \Rightarrow \exists(e \oplus e')$.

4.5.1. (Существование конечных ортогональных прямых сумм.) Из **4.2.4** немедленно следует, что в устойчивых моноидах существуют прямые суммы произвольных конечных ортогональных семейств идемпотентов.

4.5.2. (Мультипликативный моноид кольца устойчив.) Если A — коммутативное кольцо, то его мультипликативный моноид A^\times устойчив. В самом деле, для любых двух ортогональных идемпотентов $e, e' \in A$ в качестве $e \oplus e'$ можно взять их сумму $e + e'$. Таким образом, структура мультипликативного моноида A^\times определяет сложение для некоторых пар элементов, а именно, для пар ортогональных идемпотентов.

Определение 4.6 (Моноиды с ортогональным дополнением.) Пусть M — коммутативный моноид с нулем. Мы говорим, что $e^\perp \in \text{Idem}(M)$ является ортогональным дополнением $e \in \text{Idem}(M)$, если $1 = e \oplus e^\perp$. Мы говорим, что M — моноид с ортогональным дополнением, если такой e^\perp существует для всех $e \in \text{Idem}(M)$.

4.6.1. (Если ортогональное дополнение e^\perp существует, то оно единственно.) Пусть e' и e'' — два ортогональных дополнения к e : $1 = e \oplus e' = e \oplus e''$. Тогда $ee' = ee'' = 0$ по **4.4.1**, и потому $e' = e' \cdot 1 = e'(e \oplus e'') = e'e \oplus e'e'' = 0 \oplus e'e'' = e'e''$ согласно **4.2.2** и **4.2.3**. Аналогично доказывается $e'' = e'e''$, и потому $e'' = e'e'' = e'$.

4.6.2. ($e \mapsto e^\perp$ — инволюция.) Поскольку $1 = e \oplus e^\perp$ эквивалентно $1 = e^\perp \oplus e$, мы видим, что $(e^\perp)^\perp = e$, т.е. $e \mapsto e^\perp$ — инволюция на $\text{Idem}(M)$.

4.6.3. (Ортогональное дополнение является дополнением.) Докажем, что e^\perp является дополнением к e в полурешетке $\text{Idem}(M)$, т.е. наибольшим среди всех идемпотентов e' , таких, что $ee' = 0$. В самом деле, мы уже знаем, что $ee^\perp = 0$; и если $ee' = 0$, то $e' = e' \cdot 1 = e'(e \oplus e^\perp) = e'e \oplus e'e^\perp = 0 \oplus e'e^\perp = e'e^\perp$, т.е. $e' \leq e^\perp$.

Отсюда, в частности, следует, что $e \rightarrow e^\perp$ обращает порядок на полурешетке $\text{Idem}(M)$, и что $\text{Idem}(M)$ — решетка для любого моноида с ортогональными дополнениями: в качестве $e \vee e'$ можно взять $(e^\perp \cdot e'^\perp)^\perp$.

Кроме того, заметим, что инволюция $e \rightarrow e^\perp$ зависит только от полурешетки $\text{Idem}(M)$.

4.6.4. (Мультипликативный моноид кольца обладает ортогональными дополнениями.) Если $M = A^\times$ для некоторого кольца A , то e^\perp существует для любого идемпотента $e \in \text{Idem}(M) = \text{Idem}(A)$ и равен $1 - e$. Таким образом, мультипликативный моноид кольца всегда является устойчивым моноидом с ортогональным дополнением.

Определение 4.7 (Устойчивые идеалы в $\text{Idem}(M)$ и M). Пусть M — устойчивый моноид, $\mathfrak{a} \subset \text{Idem}(M)$ — идеал в моноиде $\text{Idem}(M)$. Мы говорим, что \mathfrak{a} — устойчивый идеал в $\text{Idem}(M)$, если вместе с любыми двумя ортогональными идемпотентами он содержит их ортогональную прямую сумму. Мы говорим, что $\mathfrak{b} \subset M$ — устойчивый идемпотентный идеал, если \mathfrak{b} порождается некоторым устойчивым идеалом $\mathfrak{a} \subset \text{Idem}(M)$.

4.7.1. (Идеалы $\mathfrak{a} \subset M$ и $\mathfrak{b} \subset \text{Idem}(M)$ определяют друг друга.) Заметим, что $\mathfrak{b} = M\mathfrak{a}$ и $\mathfrak{a} = \mathfrak{b} \cap \text{Idem}(M)$, поэтому \mathfrak{a} и \mathfrak{b} определяют друг друга.

Теорема 4.8 (Устойчивые идемпотентные идеалы в кольце.) Пусть A — коммутативное кольцо. Тогда идеалы кольца A , порожденные содержащимися в них идемпотентами — это в точности устойчивые идемпотентные идеалы в мультипликативном моноиде A .

Доказательство. Пусть $S \subset \text{Idem}(A)$ — произвольное множество идемпотентов, \mathfrak{a} — наименьший устойчивый идеал в $\text{Idem}(A)$, содержащий S , $\mathfrak{b} = A^\times \mathfrak{a}$ — наименьший устойчивый идемпотентный идеал в A^\times , содержащий S , $\mathfrak{c} = A \cdot S$ — идеал кольца A , порожденный S . Мы хотим доказать, что $\mathfrak{b} = \mathfrak{c}$.

Поскольку \mathfrak{c} замкнут относительно сумм любых элементов (и, в частности, ортогональных сумм идемпотентов) и устойчив относительно умножения на любые элементы A , мы видим, что $\mathfrak{c} \supset \mathfrak{a}$ и что \mathfrak{c} порождается \mathfrak{a} как идеал кольца A , откуда $\mathfrak{c} \supset \mathfrak{b} = A^\times \mathfrak{a} \supset \mathfrak{a}$. Докажем, что множество $\mathfrak{b} \subset A$ замкнуто относительно сложения; отсюда будет следовать $\mathfrak{c} = \mathfrak{b}$.

Итак, пусть $e, e' \in \mathfrak{a} \subset \text{Idem}(A)$, $x, y \in A$; мы хотим доказать, что $z := xe + ye'$ лежит в $\mathfrak{b} = A^\times \mathfrak{a}$, т.е. делится на какой-то идемпотент из \mathfrak{a} . Запишем $z = (x + ye')e + y(1 - e)e'$; мы видим, что z является линейной комбинацией ортогональных идемпотентов e и $(1 - e)e'$ из $\mathfrak{a} \subset \text{Idem}(A)$. Переобозначив $(1 - e)e'$ через e' , мы можем считать, что с самого начала $ee' = 0$. Тогда $e + e' = e \oplus e'$ также лежит в \mathfrak{a} , поскольку \mathfrak{a} устойчив, и при этом $e(e \oplus e') = e$, $e'(e \oplus e') = e'$; отсюда $z = xe + ye' = z(e \oplus e') \in \mathfrak{b} = A^\times \mathfrak{a}$, что и требовалось доказать.

Определение 4.9 (Факторизация по устойчивому идеалу.) Пусть M — устойчивый моноид с ортогональными дополнениями, $\mathfrak{b} \subset M$ — устойчивый идемпотентный идеал, $\mathfrak{a} := \mathfrak{b} \cap \text{Idem}(M)$ — соответствующий устойчивый идеал в $\text{Idem}(M)$. Рассмотрим на M отношение эквивалентности $\equiv_{\mathfrak{a}}$, определенное следующим образом: $x \equiv_{\mathfrak{a}} y$, если и только если $xe^{\perp} = ye^{\perp}$ для некоторого идемпотента $e \in \mathfrak{a}$. Обозначим через $M/\mathfrak{a}M$ или M/\mathfrak{b} фактормножество M по этому отношению эквивалентности; оно является моноидом, и мы будем говорить, что M/\mathfrak{b} есть фактормоноид M по устойчивому идемпотентному идеалу \mathfrak{b} .

4.9.1. ($\equiv_{\mathfrak{a}}$ есть отношение эквивалентности.) Несложно видеть, что $\equiv_{\mathfrak{a}}$ — отношение эквивалентности. В самом деле, $xe^{\perp} = ye^{\perp}$ влечет $xe'^{\perp} = ye'^{\perp}$ для любого идемпотента $e' \geq e$, поскольку $e^{\perp}e'^{\perp} = e'^{\perp}$. Поэтому если $xe^{\perp} = ye^{\perp}$ и $ye'^{\perp} = ze'^{\perp}$, то $x(e \vee e')^{\perp} = y(e \vee e')^{\perp} = z(e \vee e')^{\perp}$. Осталось заметить, что если $e, e' \in \mathfrak{b}$, то и $e \vee e' \in \mathfrak{b}$, поскольку $e \vee e' = e \vee (e'(e \oplus e^{\perp})) = e \vee (e'e \oplus e'e^{\perp}) = e \vee e'e \vee e'e^{\perp} = e \vee e'e^{\perp} = e \oplus e'e^{\perp}$, e и $e'e^{\perp}$ ортогональны, а \mathfrak{b} — устойчивый идеал.

4.9.2. (Устойчивый идеал — это идеал в $\text{Idem}(M)$, замкнутый относительно конечных верхних граней.) Только что проделанное рассуждение показывает, что идеал $\mathfrak{a} \subset \text{Idem}(M)$ устойчив если и только если он замкнут относительно операции \vee , т.е. является подрешеткой в $\text{Idem}(M)$.

4.9.3. (Альтернативное описание M/\mathfrak{b} .) Несложно видеть, что фактормножество M/\mathfrak{b} может быть записано как индуктивный предел идемпотентных фактормоноидов Me^{\perp} (рассматриваемых как фактормножества M), взятый по частично упорядоченному множеству $e \in \mathfrak{a} = \text{Idem}(M) \cap \mathfrak{b}$. Этот индуктивный предел фильтруется, поскольку \mathfrak{a} замкнуто относительно \vee ; поэтому этот индуктивный предел одновременно будет и индуктивным пределом моноидов Me^{\perp} , а значит, M/\mathfrak{b} будет моноидом, фактормоноидом исходного моноида M по отношению эквивалентности $\equiv_{\mathfrak{a}}$.

Теорема 4.10 (Факторизация кольца по устойчивому идеалу.) Пусть A — кольцо, $\mathfrak{a} \subset \text{Idem}(A)$ — устойчивый идеал, $\mathfrak{b} = A\mathfrak{a} = A^{\times}\mathfrak{a}$ — соответствующий идеал кольца A . Тогда отображение $A \rightarrow A/\mathfrak{b} = A/\equiv_{\mathfrak{a}}$, построенное согласно 4.9, может быть отождествлено с отображением кольца A в факторкольцо по идеалу \mathfrak{b} . Иначе говоря, $x \equiv_{\mathfrak{a}} y$ если и только если $x - y \in A\mathfrak{b}$.

Доказательство. Запишем снова $A/\equiv_{\mathfrak{a}}$ как фильтрующийся индуктивный предел моноидов $Ae^{\perp} = A(1 - e)$ по $e \in \mathfrak{a}$. Поскольку все отображения перехода в этой диаграмме являются гомоморфизмами колец, и

к тому же $Ae^\perp = A(1 - e)$ может быть отождествлено с факторкольцом A/Ae , мы видим, что $A/\equiv_{\mathfrak{a}}$ есть кольцо, индуктивный предел факторколец A/Ae по $e \in \mathfrak{a}$, т.е. факторкольцо A по объединению (индуктивному пределу) всех таких Ae . Это объединение и есть в точности идеал \mathfrak{b} .

Определение 4.11 (Максимальные устойчивые идеалы.) Пусть M — устойчивый моноид. Идеал $\mathfrak{m} \subset \text{Idem}(M)$ называется максимальным устойчивым идеалом, если он максимален по включению среди всех устойчивых идеалов $\text{Idem}(M)$, отличных от единичного. Аналогично, $\mathfrak{m}' \subset M$ называется максимальным устойчивым идемпотентным идеалом, если он максимален среди всех таких идеалов моноида M , отличных от единичного. Между такими \mathfrak{m} и \mathfrak{m}' есть взаимно однозначное соответствие, задаваемое формулами $\mathfrak{m} \mapsto M\mathfrak{m}$ и $\mathfrak{m}' \mapsto \mathfrak{m}' \cap \text{Idem}(M)$.

4.11.1. (Существование максимальных устойчивых идеалов.) Как обычно, если M — нетривиальный устойчивый моноид, то из леммы Цорна следует существование хотя бы одного максимального устойчивого идеала \mathfrak{m} в $\text{Idem}(M)$.

Теорема 4.12 (Фактормоноид по максимальному устойчивому идеалу связан.) Пусть M — устойчивый моноид с ортогональными дополнениями, $\mathfrak{m} \subset \text{Idem}(M)$ — максимальный устойчивый идеал. Тогда моноид $M/\mathfrak{m}M$ связан, т.е. $\text{Idem}(M/\mathfrak{m}M) = \{0, 1\}$.

Доказательство. Заметим, что $1 \neq 0$ в $M/\mathfrak{m}M$, т.е. $1 \not\equiv_{\mathfrak{m}} 0$: в противном случае было бы $1 \cdot e^\perp = 0 \cdot e^\perp$ для некоторого $e \in \mathfrak{m}$, т.е. $e^\perp = 0$ и $e = 1$, что противоречит $\mathfrak{m} \neq \text{Idem}(M)$.

Пусть $\bar{e} \in \text{Idem}(M/\mathfrak{m}M)$. Поскольку $M/\mathfrak{m}M = \varinjlim_{e \in \mathfrak{m}} Me^\perp$, существует элемент $e' \in \mathfrak{m}$ и представитель $e \in \text{Idem}(Me'^\perp)$ идемпотента \bar{e} , так что $e \leq e'^\perp$ и $ee' = 0$. Если $e \in \mathfrak{m}$, то $e'' = e \oplus e'$ также лежит в \mathfrak{m} , поскольку \mathfrak{m} устойчив, и потому образ e в Me''^\perp равен $e(e \oplus e')^\perp = ee^\perp e'^\perp = 0$; тем более $\bar{e} = 0$ в $M/\mathfrak{m}M$.

Рассмотрим теперь случай $e \notin \mathfrak{m}$. Пусть $\mathfrak{m}_e := (\mathfrak{m} : e) = \{\tilde{e} \in \text{Idem}(M) : e\tilde{e} \in \mathfrak{m}\}$. Тогда $\mathfrak{m}_e \supset \mathfrak{m}$ — идеал в $\text{Idem}(M)$, не содержащий единицу и устойчивый из-за дистрибутивности ортогональных прямых сумм. Из максимальной \mathfrak{m} получаем $\mathfrak{m}_e = \mathfrak{m}$. В частности, $ee^\perp = 0 \in \mathfrak{m}$, и потому $e^\perp \in \mathfrak{m}_e = \mathfrak{m}$, и, следовательно, $e_1 := e^\perp \vee e' = e^\perp \oplus ee'$ лежит в \mathfrak{m} . Рассмотрим образ e в Me_1^\perp : поскольку $e^\perp \leq e_1$, верно также $e \geq e_1^\perp$, а значит, $ee_1^\perp = e_1^\perp$, т.е. этот образ равен единице Me_1^\perp ; тем более образ e в $M/\mathfrak{m}M$ равен единице.

4.13. (Применение к нашей задаче: можно считать A и B связными.)
Итак, пусть A — нетривиальная целая \mathbb{F}_p -алгебра, B — нетривиальная целая \mathbb{F}_ℓ -алгебра, $\theta : A^\times \xrightarrow{\sim} B^\times$ — мультипликативный изоморфизм. Выберем в моноиде $\text{Idem}(M)$, где $M := A^\times$, максимальный идемпотентный идеал \mathfrak{m} . Поскольку все наши конструкции были проделаны на уровне моноидов, $\theta(\mathfrak{m})$ — максимальный идеал в $\text{Idem}(B^\times)$, θ переводит отношение эквивалентности $\equiv_{\mathfrak{m}}$ в $\equiv_{\theta(\mathfrak{m})}$, и индуцирует изоморфизм $\bar{\theta} : \bar{A}^\times \rightarrow \bar{B}^\times$, где $\bar{A} := A / \equiv_{\mathfrak{m}}$ можно отождествить с факторалгеброй $A/\mathfrak{m}A$, а $\bar{B} := B / \equiv_{\theta(\mathfrak{m})}$ — с факторалгеброй $B/\theta(\mathfrak{m})B$. Поскольку \bar{A} и \bar{B} — связные нетривиальные алгебры тех же характеристик p и ℓ , мы можем заменить A и B на \bar{A} и \bar{B} и считать эти алгебры *связными*: $\text{Idem}(A) = \{0, 1\}$. При этом они по-прежнему останутся целыми над простыми подкольцами.

4.13.1. (Связная целая алгебра над полем k локальна с алгебраическим полем вычетов.) Заметим, что связная целая коммутативная алгебра A над полем k автоматически локальна. В самом деле, гомоморфизм $A \rightarrow A/\mathfrak{n}_A$ индуцирует биекцию между $\text{Idem}(A)$ и $\text{Idem}(A/\mathfrak{n}_A)$ (согласно лемме Гензеля, любое решение сепарабельного уравнения $e^2 = e$ в A/\mathfrak{n}_A можно поднять до единственного решения в A), поэтому A/\mathfrak{n}_A связна. С другой стороны, A/\mathfrak{n}_A — целая приведенная k -алгебра, любая конечнопорожденная подалгебра которой также является целой, приведенной и связной, а значит — полем, конечным расширением поля k . Отсюда следует, что A/\mathfrak{n}_A является фильтрующимся индуктивным пределом полей, конечных расширений поля k , а значит, само является некоторым полем K , алгебраическим над k . Поскольку нильрадикал \mathfrak{n}_A содержится во всех максимальных идеалах A , мы видим, что он является единственным максимальным идеалом кольца A , т.е. A — локальное кольцо, поле вычетов которого алгебраично над полем k , а максимальный идеал совпадает с нильрадикалом.

5 Редукция к случаю алгебраических расширений

Итак, теперь у нас A — связная целая \mathbb{F}_p -алгебра, или, что, как мы только что выяснили, одно и то же — локальная \mathbb{F}_p -алгебра с максимальным нильрадикалом $\mathfrak{m}_A = \mathfrak{n}_A$ и алгебраическим полем вычетов $K := A/\mathfrak{m}_A \supset \mathbb{F}_p$, и, аналогично, B — связная целая \mathbb{F}_ℓ -алгебра, которая является локальной \mathbb{F}_ℓ -алгеброй с алгебраическим полем вычетов $L := B/\mathfrak{m}_B \supset \mathbb{F}_\ell$ и максимальным нильрадикалом $\mathfrak{m}_B = \mathfrak{n}_B$.

По-прежнему у нас задан мультипликативный изоморфизм $\theta : A^\times \rightarrow B^\times$.

Мы хотим доказать, что в такой ситуации обязательно $\mathfrak{m}_A = 0$, $\mathfrak{m}_B = 0$, т.е. $A = K$ и $B = L$ являются полями, алгебраическими расширениями \mathbb{F}_p и \mathbb{F}_ℓ соответственно.

5.1. (Структура обратимых элементов в A .) Заметим, что элемент локального кольца A обратим, если и только если его образ в $A/\mathfrak{m}_A = K$ обратим. Отсюда получаем короткую точную последовательность абелевых групп:

$$1 \rightarrow (1 + \mathfrak{m}_A)^\times \rightarrow A^* \rightarrow K^* \rightarrow 1 \quad (5.1.1)$$

Порядок любого элемента K^* взаимно прост с p ; напротив, порядок любого элемента $1 + u \in (1 + \mathfrak{m}_A)^\times$ является степенью p , поскольку из $u^{p^k} = 0$ следует $(1 + u)^{p^k} = 1$. Таким образом, $(1 + \mathfrak{m}_A)^\times$ является p -примарной частью A^* , а K^* — взаимно простой с p . В действительности представители Тейхмюллера дают нам мультипликативное сечение проекции $A \rightarrow K$, так что $A^* = (1 + \mathfrak{m}_A)^\times \times A_{p\text{-red}}^* \cong (1 + \mathfrak{m}_A)^\times \times K^*$.

5.1.1. (Корни из единицы в A .) Обозначим через c_n количество корней n -ой степени из единицы в A , или, что то же самое, в B :

$$c_n = |\mu_n(A)| = |\mu_n(B)| \quad (5.1.2)$$

Мы будем использовать обозначение $\mu_n(M)$ для множества “корней n -ой степени из единицы” в любом коммутативном моноиде M :

$$\mu_n(M) = \{x \in M : x^n = 1\} \quad (5.1.3)$$

Очевидно, $c_n = c_{n'}c_{n''}$, если $n = n'n''$ и числа n' и n'' взаимно просты, поскольку в этом случае $\mu_n = \mu_{n'} \times \mu_{n''}$. Поэтому достаточно выяснить, чему равно c_n для случая, когда n — степень простого.

5.1.2. (Формула для c_n .) Поскольку $A^* \cong K^* \times (1 + \mathfrak{m}_A)^*$, мы видим, что $c_n = |\mu_n(K)| \cdot |\mu_n((1 + \mathfrak{m}_A)^\times)|$. Если n взаимно просто с p , то $c_n = |\mu_n(K)| \leq n$, поскольку $(1 + \mathfrak{m}_A)^\times$ p -примарна, а K — поле.

5.1.3. ($c_n \leq n$.) Докажем, что $c_n \leq n$ для любого натурального n . Достаточно доказать это для $n = q^a$, где q — простое число. Если $q \neq p$, то $c_n = |\mu_n(K)| \leq n$, поскольку K — поле. Если же $q = p$, то $q \neq \ell$, и потому $c_n = |\mu_n(L)| \cdot |\mu_n((1 + \mathfrak{m}_B)^\times)| = |\mu_n(L)| \leq n$ благодаря изоморфизму θ . Таким образом, $c_n \leq n$ для всех n .

5.2. ($c_p \leq p$: последствия для структуры A .) Заметим, в частности, что $c_p \leq p$, т.е. $|\mu_p((1 + \mathfrak{m}_A)^\times)| = |\mu_p(A)| = c_p \leq p$ (мы воспользовались тем, что $\mu_p(K) = 1$, поскольку K — поле характеристики p). Иначе говоря, не более чем p элементов $(1 + \mathfrak{m}_A)^\times$ аннулируются возведением в p -ую степень.

5.2.1. (Случай $\mathfrak{m}_A \neq 0$: обязательно $K = \mathbb{F}_p$.) Предположим, $\mathfrak{m}_A \neq 0$. Выберем какой-нибудь нильпотент $\varepsilon \neq 0$ из \mathfrak{m}_A ; можно считать, что $\varepsilon^p = 0$ (иначе заменим ε на $\varepsilon^{p^{k-1}}$, где k — наименьшее число, для которого $\varepsilon^{p^k} = 0$). В таком случае все элементы вида $1 + x\varepsilon$ попадают в $\mu_p((1 + \mathfrak{m}_A)^\times)$, а значит, существует не более p таких элементов. Однако если брать в качестве x представители Тейхмюллера элементов из K (т.е. $x \in A_{p\text{-red}}$), то все $1 + x\varepsilon$ будут различны (поскольку разность любых двух различных представителей Тейхмюллера обратима), а значит, получим не менее $\text{card } K$ различных элементов из $\mu_p(A)$. Отсюда $\text{card } K \leq \text{card } \mu_p(A) = c_p \leq p$, однако $K \supset \mathbb{F}_p$, откуда $\text{card } K \geq p$. Из этой цепочки неравенств получаем $K = \mathbb{F}_p$ и $c_p = p$. Кроме того, оказывается, что элементы $1 + x\varepsilon$ — это все корни p -ой степени из единицы в A .

5.2.2. (Структура корней p -ой степени из нуля.) Пусть $\mathfrak{n} := \{\varepsilon \in A : \varepsilon^p = 0\} \subset \mathfrak{m}_A$. Поскольку A — \mathbb{F}_p -алгебра, \mathfrak{n} — идеал в A , и, в частности, \mathbb{F}_p -векторное пространство. Кроме того, элементы \mathfrak{n} взаимно однозначно соответствуют корням p -ой степени из единицы $\mu_p(A)$ с помощью отображения $u \mapsto 1 + u$, и мы уже выяснили, что $\text{card } \mathfrak{n} = c_p = p$. Иначе говоря, \mathfrak{n} — одномерное \mathbb{F}_p -векторное пространство. В частности, любые два ненулевых элемента \mathfrak{n} отличаются умножением на некоторый элемент \mathbb{F}_p^* .

5.2.3. ($\mathfrak{m}_A \mathfrak{n} = 0$.) Докажем теперь, по-прежнему предполагая $\mathfrak{m}_A \neq 0$, что $\mathfrak{m}_A \mathfrak{n} = 0$. Пусть $\varepsilon \in \mathfrak{n}$, $\eta \in \mathfrak{m}_A$, $\varepsilon \neq 0$, $\eta \neq 0$; проверим, что $\varepsilon\eta = 0$. Тогда $\varepsilon^p = 0$, а значит, $(\varepsilon\eta)^p = 0$, т.е. $\varepsilon\eta \in \mathfrak{n}$. Поскольку \mathfrak{n} — одномерное \mathbb{F}_p -векторное пространство, $\varepsilon\eta = c\varepsilon$ для некоторого $c \in \mathbb{F}_p$. Если $c = 0$, то получаем требуемое равенство $\varepsilon\eta = 0$; если же $c \in \mathbb{F}_p^*$, то $\varepsilon(c - \eta) = 0$, и элемент $c - \eta$ обратим в A , следовательно, $\varepsilon = 0$, что противоречит предположению.

5.2.4. (Все нильпотенты $\varepsilon \in \mathfrak{m}_A$ аннулируются возведением в p -ую степень; \mathfrak{m}_A конечно.) Пусть теперь $\varepsilon \in \mathfrak{m}_A$ — произвольный нильпотент, и пусть n — наименьшее натуральное число, для которого $\varepsilon^n = 0$. Тогда $(\varepsilon^{\lceil n/p \rceil})^p = 0$, т.е. $\varepsilon^{\lceil n/p \rceil} \in \mathfrak{n}$, откуда $\varepsilon^{\lceil n/p \rceil + 1} = \varepsilon \cdot \varepsilon^{\lceil n/p \rceil} \in \mathfrak{m}_A \mathfrak{n} = 0$ по предыдущему пункту. Согласно выбору n , должно быть $\lceil n/p \rceil + 1 \geq n$, откуда $(n+1)/2 + 1 \geq \lceil n/2 \rceil + 1 \geq \lceil n/p \rceil + 1 \geq n$ и $n \leq 3$. Если $p \geq 3$, мы видим, что $\varepsilon^p = 0$, т.е. $\mathfrak{m}_A \subset \mathfrak{n}$, и, в частности, \mathfrak{m}_A конечно и состоит из p элементов. Если же $p = 2$, то мы видим, что \mathfrak{m}_A есть множество $\{\varepsilon : \varepsilon^4 = 0\}$ корней четвертой степени из нуля, элементы которого состоят во взаимно однозначном соответствии с $\mu_4(A)$ посредством отображения $u \mapsto 1 + u$. Поэтому $\text{card } \mathfrak{m}_A = \text{card } \mu_4(A) = c_4 \leq 4$, т.е. и в этом случае \mathfrak{m}_A конечно.

5.2.5. (Если $\mathfrak{m}_A \neq 0$, то A и B конечны.) Мы видим, что если $\mathfrak{m}_A \neq 0$,

то $A/\mathfrak{m}_A = \mathbb{F}_p$ конечно, и подгруппа \mathfrak{m}_A также конечна (и состоит из не более чем p^2 элементов). Поэтому в этом случае кольцо A конечно, а значит, это же верно и для B ввиду существования биекции θ .

5.2.6. (Обязательно $\mathfrak{m}_A = \mathfrak{m}_B = 0$.) Осталось заметить, что если A и B конечны, то количество элементов в A есть степень простого числа p (поскольку A — \mathbb{F}_p -алгебра), а количество элементов B есть степень другого простого числа ℓ . Биекция $\theta : A^\times \rightarrow B^\times$ приводит к равенству $p^{\dim A} = |A| = |B| = \ell^{\dim B}$, которое невозможно для ненулевых A и B . Таким образом, предположение $\mathfrak{m}_A \neq 0$ приводит к противоречию, и, конечно же, это же верно и для $\mathfrak{m}_B \neq 0$.

5.2.7. ($A = K$ и $B = L$ — поля, алгебраические расширения \mathbb{F}_p и \mathbb{F}_ℓ .) Мы доказали, что $\mathfrak{m}_A = 0$ и $\mathfrak{m}_B = 0$, откуда $A = A/\mathfrak{m}_A = K$ — поле, алгебраическое расширение \mathbb{F}_p , и аналогично $B = L$ — поле, алгебраическое расширение \mathbb{F}_ℓ .

6 Сверхнатуральные числа и алгебраические расширения конечных полей

Нам осталось выяснить, при каких p и ℓ существуют алгебраические расширения K и L полей \mathbb{F}_p и \mathbb{F}_ℓ соответственно, обладающие изоморфными мультипликативными группами: $K^* \xrightarrow{\sim} L^*$. Для этого нам надо классифицировать алгебраические расширения конечных полей.

Определение 6.1 (Сверхнатуральные числа $\bar{\mathbb{N}}$.) Пусть $\mathbb{N} = \mathbb{N}^\times$ — натуральные числа, рассматриваемые как коммутативный моноид по умножению, упорядоченный отношением делимости. Обозначим через $\bar{\mathbb{N}}$ частично упорядоченный моноид, получающийся из \mathbb{N} пополнением относительно операции вычисления наименьшего общего кратного (т.е. верхней грани) произвольных подмножеств. Мы говорим, что $\bar{\mathbb{N}}$ — моноид сверхнатуральных чисел, а его элементы называем сверхнатуральными числами. Если сверхнатуральное число принадлежит $\mathbb{N} \subset \bar{\mathbb{N}}$, мы называем его конечным.

Существует несколько эквивалентных описаний сверхнатуральных чисел, каждое из которых могло бы быть принято за определение.

6.1.1. (Описание сверхнатуральных чисел через множества конечных делителей.) Несложно видеть, что любое сверхнатуральное число x является наименьшим общим кратным множества своих конечных делителей

$D_x \subset \mathbb{N}$. Можно использовать это для построения $\bar{\mathbb{N}}$, определив сверхнатуральное число как подмножество $D \subset \mathbb{N}$, устойчивое относительно перехода к делителям и взятия конечных н.о.к. При этом натуральному числу n сопоставляется множество его делителей D_n ; произведение двух множеств $D, D' \subset \mathbb{N}$ определяется как множество произведений DD' ; отношение делимости есть просто включение множеств, и н.о.к. произвольного семейства множеств вычисляется через взятие их объединения, а затем — добавления к нему делителей н.о.к. любых его конечных подмножеств.

6.1.2. (Описание сверхнатуральных чисел через их разложения на простые.) Альтернативное описание: сверхнатуральные числа — это бесконечные произведения $2^{\nu_1} 3^{\nu_2} 5^{\nu_3} \dots p_k^{\nu_k} \dots$, где показатели $\nu_k \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ могут принимать целые неотрицательные или бесконечные значения. Видно, что $\bar{\mathbb{N}} \cong (\mathbb{Z}_{\geq 0} \cup \{\infty\})^{\mathbb{P}}$, и понятно, как именно натуральные числа вкладываются в сверхнатуральные. Этот подход принят в основополагающей работе Штейница по теории полей [St1910], а также в книге Серра [Se64].

Из этого описания видно, что частичный порядок на $\bar{\mathbb{N}}$ — это в точности отношение делимости в $\bar{\mathbb{N}}$: $\mathbf{y} \leq \mathbf{x}$ если и только если $\mathbf{x} = \mathbf{y}\mathbf{z}$ для некоторого $\mathbf{z} \in \bar{\mathbb{N}}$.

6.1.3. (Сверхнатуральные числа как индексы замкнутых подгрупп в проконечных группах.) Определим *индекс* $(G : H)$ замкнутой подгруппы $H \subset G$ проконечной группы G как н.о.к. индексов $(G : U)$ открытых подгрупп $U \subset G$, содержащих H . Очевидно, $(G : H)$ — сверхнатуральное число, которое конечно в том и только том случае, если H открыта в G (см. также [Se64]).

6.1.4. (Сверхнатуральные числа как степени алгебраических расширений.) Аналогично, определим *степень* $[L : K]$ алгебраического расширения L поля K как н.о.к. степеней $[F : K]$ всех конечных расширений F поля K , содержащихся в L (см. [St1910]). Конечно же, для сепарабельного L/K степень $[L : K]$ равна индексу замкнутой подгруппы $\text{Gal}(\bar{K}/L)$ в группе Галуа $\text{Gal}(\bar{K}/K)$.

Теорема 6.2 (Классификация алгебраических расширений конечного поля; ср. [St1910, III.16].)

- а) Соответствие $H \mapsto (\hat{\mathbb{Z}} : H)$ определяет биекцию между замкнутыми подгруппами $H \subset \hat{\mathbb{Z}}$ и сверхнатуральными числами $\mathbf{x} \in \bar{\mathbb{N}}$. При этом отношение включения переходит в отношение делимости.

- б) Соответствие $L \mapsto [L : \mathbb{F}_q]$ определяет биекцию между алгебраическими расширениями L конечного поля \mathbb{F}_q , содержащимися в фиксированном алгебраическом замыкании $\bar{\mathbb{F}}_q$ поля \mathbb{F}_q , и сверхнатуральными числами. При этом отношение включения соответствует отношению делимости.
- с) Два алгебраических расширения \mathbb{F}_q изоморфны если и только если равны их степени.

Доказательство. а) следует из того, что открытые подгруппы $\hat{\mathbb{Z}}$ — это в точности подгруппы вида $n\hat{\mathbb{Z}}$, они однозначно определяются своим индексом $n = (\hat{\mathbb{Z}} : n\hat{\mathbb{Z}})$, и $n\hat{\mathbb{Z}} \subset m\hat{\mathbb{Z}}$ если и только если m делит n , а также из того, что замкнутая подгруппа $H \subset \hat{\mathbb{Z}}$ является пересечением всех открытых подгрупп, ее содержащих, а значит, однозначно восстанавливается по их набору. Утверждение б) следует из а) с помощью теории Галуа; можно также явно восстановить L по его степени $\mathbf{x} = [L : \mathbb{F}_q]$, взяв композит всех расширений \mathbb{F}_{q^f} по конечным делителям f сверхнатурального числа \mathbf{x} . Для доказательства с) можно сначала вложить оба алгебраических расширения в одно и то же алгебраическое замыкание $\bar{\mathbb{F}}_q$, а затем применить б).

6.2.1. (Применение к нашей задаче.) Таким образом, вместо того, чтобы задавать алгебраическое расширение K поля \mathbb{F}_p и алгебраическое расширение L поля \mathbb{F}_ℓ , нам достаточно задать их степени $\mathbf{x} := [K : \mathbb{F}_p]$ и $\mathbf{y} := [L : \mathbb{F}_\ell]$. Однако нам теперь надо выяснить, как устроена мультипликативная группа K^* , в зависимости от характеристики p и степени \mathbf{x} .

Определение 6.3 (Инд-циклические группы.) Мы будем говорить, что абелева группа A инд-циклическа, если она является фильтрующим индуктивным пределом конечных циклических групп, или, что одно и то же, если любые два элемента группы A лежат в некоторой конечной циклической подгруппе.

6.3.1. (Альтернативное описание.) Несложно видеть, что абелева группа A инд-циклическа если и только если она является группой кручения, и $\text{card } \mu_n(A) \leq n$ для всех натуральных n . Как обычно, из этого неравенства индукцией по n выводится, что все подгруппы $\mu_n(A)$ циклически и одновременно — что количество элементов порядка n равно 0 или $\varphi(n)$, и потому $A = \varinjlim_n \mu_n(A)$ инд-циклическа. Обратная импликация очевидна: если A инд-циклическа, то ее подгруппа $\mu_n(A)$ инд-циклическа и аннулируется n , откуда немедленно следует, что она порождается любым своим элементом максимального порядка (который не может превосходить n).

6.3.2. (Примеры.) Группа корней из единицы $\mu_\infty(K)$ в произвольном поле K является инд-циклической. Группа $\mathbb{Q}/\mathbb{Z} = \varinjlim_n \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ инд-циклическа.

6.3.3. (Свойства инд-циклических групп.) Из определения немедленно следует, что любая подгруппа и факторгруппа инд-циклической группы инд-циклическа, и что конечная группа инд-циклическа тогда и только тогда, когда она циклическа. Можно доказать, что любая инд-циклическая группа A вкладывается в качестве подгруппы в \mathbb{Q}/\mathbb{Z} , и что образ этого вложения, но не само вложение, однозначно определяется группой A . Образ любого вложения $A \rightarrow \mathbb{Q}/\mathbb{Z}$ может быть охарактеризован как множество тех элементов \mathbb{Q}/\mathbb{Z} , порядок которых совпадает с порядком какого-нибудь элемента A . Само вложение строится по индукции: для каждого n определяется гомоморфизм $\varphi_n : \mu_{n!}(A) \rightarrow \frac{1}{n!}\mathbb{Z}/\mathbb{Z}$, продолжающий φ_{n-1} , после чего берется индуктивный предел всех φ_n .

6.3.4. (Порядок инд-циклической группы.) Определим *порядок* $o(A) \in \bar{\mathbb{N}}$ инд-циклической группы A как н.о.к. порядков всех ее элементов. Несложно видеть, что A однозначно определяется своим порядком $o(A)$, поскольку она (неканонически) изоморфна подгруппе \mathbb{Q}/\mathbb{Z} , состоящей из тех элементов, порядок которых делит $o(A)$. Наоборот, каждому сверхнатуральному числу x можно сопоставить подгруппу $(\mathbb{Q}/\mathbb{Z})_x \subset \mathbb{Q}/\mathbb{Z}$, состоящую из тех элементов, порядок которых делит x ; порядок построенной таким образом инд-циклической группы равен x .

Таким образом, порядок инд-циклической группы определяет биекцию между множеством классов изоморфности инд-циклических групп и сверхнатуральными числами.

6.3.5. (Порядок K^* как функция $\text{char } K = p$ и степени $[K : \mathbb{F}_p]$.) Пусть K — алгебраическое расширение поля \mathbb{F}_p . Тогда группа K^* состоит из корней из единицы, и потому инд-циклическа. Ее класс изоморфности определен сверхнатуральным числом $o(K^*)$, поэтому мультипликативные моноиды алгебраических расширений K/\mathbb{F}_p и L/\mathbb{F}_ℓ изоморфны если и только если $o(K^*) = o(L^*) \in \bar{\mathbb{N}}$. Теперь нам осталось научиться вычислять $o(K^*)$ через характеристику $p = \text{char } K$ и степень $x = [K : \mathbb{F}_p] \in \bar{\mathbb{N}}$.

Определение 6.4 (Продолжение функций с натуральных чисел на сверхнатуральные.) Пусть $\psi : \mathbb{N} \rightarrow \mathbb{N}$ — любая функция, сохраняющая отношение делимости (т.е. $\psi(xy)/\psi(x) \in \mathbb{N}$ для любых $x, y \in \mathbb{N}$). Мы обозначаем через $\bar{\psi} : \bar{\mathbb{N}} \rightarrow \bar{\mathbb{N}}$ продолжение функции ψ на сверхнатуральные числа, определенное следующим образом: $\bar{\psi}(x)$ есть н.о.к. значений $\psi(x)$ функции ψ на конечных делителях $x|x$ сверхнатурального числа x . Несложно видеть, что на конечных числах $\bar{\psi}$ совпадает с исходной функцией ψ , и что $\bar{\psi}$ сохраняет отношение делимости сверхнатуральных чисел; поэтому

мы будем обозначать $\bar{\psi}$ тем же символом ψ , что и исходную функцию, если это не приводит к путанице.

Определение 6.5 (Функция $a^x - 1$.) Пусть $a > 1$ — целое число. Функция $\psi_a(x) := a^x - 1$ сохраняет отношение делимости на натуральных числах, и потому продолжается до функции $\bar{\psi}_a : \bar{\mathbb{N}} \rightarrow \bar{\mathbb{N}}$, определенной на сверхнатуральных числах. Мы обозначим через $a^x - 1$ значение функции $\bar{\psi}_a(\mathbf{x})$ на сверхнатуральном числе \mathbf{x} .

Следует подчеркнуть, что выражение $a^x - 1$ является цельным символом: его нельзя понимать как разность a^x и единицы, поскольку на $\bar{\mathbb{N}}$ нет операции возведения в сверхнатуральную степень и нет вычитания.

Теорема 6.6 (Структура K^* для алгебраического расширения K/\mathbb{F}_p .) Пусть K — алгебраическое расширение поля \mathbb{F}_p степени \mathbf{x} . Тогда K^* — инд-циклическая группа порядка $p^x - 1$.

Доказательство. Конечные делители f сверхнатурального числа $\mathbf{x} = [K : \mathbb{F}_p]$ — это в точности степени конечных расширений \mathbb{F}_{p^f} , содержащихся в K , так что K есть фильтрующийся индуктивный предел всех таких \mathbb{F}_{p^f} , и потому K^* есть фильтрующийся индуктивный предел циклических групп $\mathbb{F}_{p^f}^*$ порядка $p^f - 1$ для всех $f|\mathbf{x}$. Осталось заметить, что порядок такого фильтрующегося индуктивного предела как инд-циклической группы есть н.о.к. порядков входящих в него инд-циклических групп, т.е. н.о.к. $p^f - 1$ по всем конечным делителям $f|\mathbf{x}$, т.е. в точности $p^x - 1$.

Комбинируя полученные результаты, мы получаем “основную теорему” данной работы:

Теорема 6.7 (Критерий смешиваемости характеристик.) Пусть p и ℓ — различные простые числа. Существование нетривиальной \mathbb{F}_p -алгебры A и \mathbb{F}_ℓ -алгебры B с изоморфными мультипликативными моноидами равносильно существованию в сверхнатуральных числах решений уравнения

$$p^x - 1 = \ell^y - 1, \quad \text{где } \mathbf{x}, \mathbf{y} \in \bar{\mathbb{N}}. \quad (6.7.1)$$

Более того, каждое решение (\mathbf{x}, \mathbf{y}) этого уравнения дает пример таких алгебр, если взять в качестве A алгебраическое расширение поля \mathbb{F}_p степени \mathbf{x} , а в качестве B — алгебраическое расширение поля \mathbb{F}_ℓ степени \mathbf{y} .

7 Решение уравнения $a^x - 1 = b^y - 1$

Нам хотелось бы узнать, для каких пар различных простых p и ℓ уравнение $p^x - 1 = \ell^y - 1$ разрешимо в сверхнатуральных числах.

Следующая гипотеза утверждает, что ни для каких:

Гипотеза 7.1 Пусть $a, b > 1$ — натуральные числа. Уравнение $a^x - 1 = b^y - 1$ имеет решение в сверхнатуральных числах x и y тогда и только тогда, когда у него есть решение в натуральных числах, т.е. тогда и только тогда, когда $\log a / \log b \in \mathbb{Q}$.

К сожалению, пока мы не умеем доказывать это утверждение. Однако для каждой пары конкретных a и b с несоизмеримыми логарифмами обычно удается проверить (вручную или на компьютере), что у уравнения $a^x - 1 = b^y - 1$ нет решений. В частности, это так для всех пар различных простых чисел, меньших ста.

Покажем, как это происходит, например, при $a = 3, b = 5$.

7.2. (Решение уравнения $3^x - 1 = 5^y - 1$.) Итак, предположим, что $3^x - 1 = 5^y - 1$. Поскольку y делится на 1, правая часть делится на $5^1 - 1 = 4$, а значит, и левая часть делится на 4, что равносильно $2|x$. Однако если x четно, то левая часть делится на $3^2 - 1 = 8$, а значит, и правая часть делится на 8, что бывает только при четном y . Далее, при четном y правая часть делится на $5^2 - 1 = 24$, и, в частности, на 3. Но левая часть не может делиться на 3, и мы пришли к противоречию. Поэтому у данного уравнения нет решений в сверхнатуральных числах.

Общий ход рассуждений всегда именно таков: мы находим все новые и новые делители чисел x, y и $a^x - 1 = b^y - 1$, постоянно переходя из одной части уравнения в другую, и через несколько шагов получаем противоречие.

8 Связь с абсолютным тензорным произведением $\mathbb{F}_p \otimes \mathbb{F}_\ell$

Покажем, каким образом задача, рассмотренная в данной работе, связана с нетривиальностью абсолютных тензорных произведений $\mathbb{F}_p \otimes \mathbb{F}_\ell$. Подробное изложение теории гиперколец и теории новых обобщенных колец выходит за рамки данной работы, поэтому мы не будем вдаваться в подробности и приводить мотивацию последующих конструкций.

Отметим лишь, что приведенное ниже определение абсолютного тензорного произведения колец в терминах гиперколец вовсе не произвольно

и является фактически частным случаем общей конструкции тензорного произведения в категории “новых обобщенных колец”, содержащей, наряду с классическими коммутативными кольцами, также рассмотренные ниже гиперкольца, необычные объекты вроде “поля из одного элемента” \mathbb{F}_1 , и многое другое. Эта теория является расширением теории “обобщенных колец” из [Du07], и тоже основана на использовании алгебраических монад; однако на этот раз обычному кольцу R сопоставляется алгебраическая монада Λ_R , такая, что $\Lambda_R\text{-mod}$ есть категория коммутативных R -алгебр, в то время как в теории (старых) обобщенных колец сопоставлялась монада Σ_R , такая, что $\Sigma_R\text{-mod}$ есть категория R -модулей.

Определение 8.1 (*Гиперкольца.*) Гиперкольцо $A = (A, 0, 1, \times, \oplus_1, \oplus_2)$ — это множество A с двумя константами 0 и 1 и тремя бинарными операциями $\times, \oplus_1, \oplus_2 : A \times A \rightarrow A$, такими, что забывание любой из операций \oplus_1 или \oplus_2 дает коммутативное ассоциативное кольцо с единицей.

Иначе говоря, гиперкольцо — это коммутативный моноид с нулем, на котором заданы два сложения, относительно любого из которых этот моноид становится кольцом. Существует также понятие n -гиперкольца, в котором моноид наделяется n сложениями $\oplus_1, \dots, \oplus_n$; оно нам сейчас не нужно.

8.1.1. (Обозначения для коммутативных колец, связанных с гиперкольцом.) Обозначим через $i_{1,*}A$ кольцо $(A, 0, 1, \times, \oplus_1)$, а через $i_{2,*}A$ — кольцо $(A, 0, 1, \times, \oplus_2)$.

Определение 8.2 (*(C, D) -гипералгебры.*) Пусть C, D — обычные коммутативные кольца. Назовем (C, D) -гипералгеброй тройку (A, f, g) , где A — гиперкольцо, $f : C \rightarrow i_{1,*}A$, $g : D \rightarrow i_{2,*}A$ — гомоморфизмы колец. Иначе говоря, (C, D) -гипералгебра — это коммутативный моноид с двумя сложениями, наделенный структурой C -алгебры относительно первого из них и D -алгебры — относительно второго из них.

Определение 8.3 (*Абсолютное тензорное произведение $C \otimes D$.*) Обозначим через $C \otimes D$ или $C \otimes_{\mathbb{F}_1} D$ абсолютное тензорное произведение коммутативных колец C и D , определяемое как инициальный объект в категории (C, D) -гипералгебр.

Можно доказать, что гиперкольцо $C \otimes D$ существует для любых C и D , и что, например, $\mathbb{Z} \otimes \mathbb{Z} \neq \mathbb{Z}$ и $\mathbb{F}_p \otimes \mathbb{F}_p \neq \mathbb{F}_p$.

8.3.1. ($C \otimes D$ -гипералгебры.) Из определения немедленно следует, что (C, D) -гипералгебры — это то же самое, что $C \otimes D$ -гипералгебры, т.е. гиперкольца, снабженные гомоморфизмом из $C \otimes D$.

8.3.2. (Нетривиальность $C \otimes D$.) В принципе гиперкольцо $C \otimes D$ может оказаться тривиальным (т.е. одноэлементным, или таким, что $1 = 0$). Из тривиального гиперкольца есть гомоморфизмы только в тривиальные гиперкольца. Поэтому $C \otimes D \neq 0$ если и только если существует хотя бы одна нетривиальная $(C \otimes D)$ -гипералгебра, или, что одно и то же, (C, D) -гипералгебра.

8.3.3. (Альтернативное описание (C, D) -гипералгебр.) Категория (C, D) -гипералгебр, очевидно, эквивалентна категории троек (A, B, θ) , где A — C -алгебра, B — D -алгебра, $\theta : A^\times \xrightarrow{\sim} B^\times$ — изоморфизм мультипликативных моноидов. В самом деле, (C, D) -гипералгебре A можно сопоставить тройку $(i_{1,*}A, i_{2,*}A, \text{id}_A)$, и наоборот, тройке (A, B, θ) можно сопоставить гиперкольцо A , умножение и первое сложение которого наследуется из кольца A , а второе сложение получается из сложения B переносом вдоль θ : $x \oplus_2 y = \theta^{-1}(\theta(x) + \theta(y))$.

8.3.4. (Критерий $C \otimes D \neq 0$.) Комбинируя предыдущие два наблюдения, мы видим, что $C \otimes D$ нетривиально если и только если существует нетривиальная C -алгебра A , D -алгебра B и мультипликативный изоморфизм $\theta : A^\times \xrightarrow{\sim} B^\times$.

Применяя это к $C = \mathbb{F}_p$ и $D = \mathbb{F}_\ell$, получаем переформулировку результата **6.7**:

Теорема 8.4 (Критерий нетривиальности $\mathbb{F}_p \otimes \mathbb{F}_\ell$.) Абсолютное тензорное произведение $\mathbb{F}_p \otimes \mathbb{F}_\ell$ нетривиально для различных простых p и ℓ если и только если уравнение $p^x - 1 = \ell^y - 1$ разрешимо в сверхнатуральных x и y .

8.4.1. (Пример: $\mathbb{F}_3 \otimes \mathbb{F}_5 = 0$.) В частности, рассуждение **7.2** показывает, что абсолютное тензорное произведение $\mathbb{F}_3 \otimes \mathbb{F}_5$ тривиально.

Если гипотеза **7.1** верна, то $\mathbb{F}_p \otimes \mathbb{F}_\ell = 0$ для любых различных p и ℓ .

Список литературы

- [Du07] N. DUROV, *New Approach to Arakelov Geometry*, Ph.D. thesis at Bonn University, available at <http://arXiv.org/abs/0704.2030> (2007).
- [Se64] Ж.-П. СЕРР, *Когомологии Галуа*, «Мир», М., 1968.
- [St1910] E. STEINITZ, *Algebraische Theorie der Körper*, Journal für die reine und angewandte Mathematik (1910), pp. 167–309.