Министерство образования Республики Беларусь
Белорусский Государственный Университет
Механико-математический факультет

Кафедра высшей алгебры и защиты информации

Бородко Никита Константинович

Многообразия Севери-Брауэра и центральные простые алгебры

Магистерская диссертация

Научный руководитель
Тихонов С. В.
доцент, кандидат физ-мат наук

Принято к защите

«____»_____2024 г.

Заведующий кафедрой высшей алгебры и защиты информации

_____ Тихонов С. В.

доцент, кандидат физ-мат наук

Минск, 2024

Оглавление

Реферат

Магистерская работа содержит 55 с., 5 рис., 32 источника.

Ключевые слова: многообразие Севери-Брауэра, центральная простая алгебра, неабелевы когомологии, гипотеза Амицура, Wolfram Mathematica.

Цель магистерской работы — обзор теории центральных простых алгебр и многообразий Севери-Брауэра.

В первой главе приводится рассуждение о природе данной работы.

Во второй главе рассматриваются вовлечённые в теорию объекты и понятия, приводятся ссылки на литературу.

Третья глава посвящена центральным простым алгебрам, приводится подробный разбор классификации кватернионов над $\mathbb{Q}$ с кодом на Wolfram Language.

В четвёртой главе обсуждаются когомологии групп и соответствие между многообразиями Севери-Брауэра и центральными простыми алгебрами.

В пятой главе приводится гипотеза Амицура о бирациональной эквивалентности и обсуждаются возможные стратегии её решения.

Рэферат

Магісцерская праца зьмяшчае 55 с., 5 від., 32 крыніцы.

Ключавыя словы: разнастайнасць Севері-Браўэра, цэнтральная простая алгебра, неабелевы кагамалогіі, гіпотэза Аміцура, Wolfram Mathematica.

Цэль магісцерскай працы — абгляд тэорыі цэнтральных простых алгебр і разнастайнасцей Севері-Браўэра.

У першай главе прыводзіцца разважанне аб сутнасці дадзенай працы.

У другой главе разгледжваюцца ўцягнутыя да тэорыі аб'екты ды паняцці, прыводзяцца спасылкі на літаратуру.

Трэцяя глава прысвечана цэнтральным простам алгебрам, прыводзіцца падрабязны разбор класіфікацыі кватэрніонаў над $\mathbb{Q}$ з кодам на Wolfram Language.

У чацвёртай главе абмяркоўваюцца кагамалогіі груп ды адпаведнасць паміж разнастайнасцямі Севері-Браўэра і цэнтральнымі простымі алгебрамі.

У пятай главе прыводзіцца гыпотэза Аміцура аб бірацыянальнай эквівалентнасці і абмяркоўваюцца магчымыя стратэгіі яе вырашэння.

Abstract

This Master's thesis contains 55 pages, 5 pictures, 32 sources.

Keywords: Severi-Brauer variety, central simple algebra, nonabelian cohomology, Amitsur hypothesis, Wolfram Mathematica.

The goal of this paper is to provide a survey to the theory of central simple algebras and Severi-Brauer varieties.

The first chapter contains the reasoning on the gist of this work.

The second chapter tackles some prerequisites to the theory with explanations and references.

The third chapter is dedicated to central simple algebras, detailed analysis of quaternion algebras over $\mathbb{Q}$ is given.

The fourth chapter deals with group cohomology and the correspondence between central simple algebras and Severi-Brauer varieties.

The fifth chapter is about hypothesis of Amitsur on birational equivalence with reasoning on possible strategies for solving.

Глава 1

Введение

Если вы читаете бумажную версию работы, то электронная доступна тут:
https://github.com/halva-s-pivom/SBVandCSA;
Двойственно, если вы читаете электронную версию, то бумажную можно получить, распечатав электронную.

1.1 О философии данной работы

Во время работы над данной магистерской диссертацией я задавался вопросом: кто её будет читать? Это важный вопрос, т.к. от этого напрямую зависит структура работы. По моему личному мнению, основанному на наблюдениях, большинство статей, книг и иных работ по математике написано вне контекста этого вопроса, и потому они обладают наиболее распространённой структурой сухой справочно-словарной выжимки, состоящей из блоков вида определение-лемма-теорема, определение-определение-теорема-лемма, и так далее в разных пропорциях, в линейном порядке. Линейный порядок текста, тем не менее, диктуется как линейностью разговорного языка (которая следует из неизбежной зависимости от времени), так и фактом его использования на бумаге (ведь даже рисунки, будучи нелинейным языком, на пронумерованной бумаге смотрятся по порядку). Очевидно, однако, что в действительности единственная линейность в математике — это порядок возникновения тех или иных идей, определений, теорем и т.д., ибо они создаются математиками, людьми, а все мы живём во времени. Ясно также, что любой труд по математике представляет собой сжатую версию происходящего и/или происходившего, ведь иначе мы бы тратили столько времени на изучение вещей, сколько они существуют в истории математики. Проблема в следующем: с одной стороны, имеется мотивация математических объектов, обусловленная порядком возникновения идей; с другой, мотивация проистекает из той или иной красоты этих объектов и взаимосвязей между ними, которая от времени и, соответственно, порядка изложения не зависит; — *как это всё сохранить в тексте*?

Данный вопрос видится мне центральной метапроблемой множества трудов по математике. Примером этой работы я пытаюсь дать частичный ответ на него. Вообще, я бы хотел не написать, а нарисовать всё происходящее на многомерной бумаге, избавиться от линейности естественного языка и условности форм, чтобы точнее отражать те незримые вездесущие взаимосвязи теории, о которой пойдёт речь. Так как это маловозможно, я выделю из этого нелинейного незримого многообразия многосвязной теории выделю следующие объекты, которые выступают в роли центров кристаллизации.

- центральная простая алгебра
- многообразие Севери-Брауэра,
- $\mathrm{H}^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathrm{PGL}_n(K))$,

- $\mathrm{H}^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\circ)$.

Я нашёл для себя любопытной связь центральных простых алгебр с формами на примере алгебр кватернионов, поэтому подробно изложил этот момент. Многообразия Севери-Брауэра получили меньше внимания с чисто геометричной стороны, т.к. нельзя объять необъятное. Что касается H^1 и H^2, я попытался изложить предшествующую мотивацию: когомологии в R-mod для понимания когомологий групп с абелевыми коэффициентами, которые служат мотивацией для обобщения на неабелевы когомологии.

Самым же интересным явлением является устройство соответствия между центральными простыми алгебрами и многообразиями Севери-Брауэра. Я бы выделил 3 вида соответствия между математическими объектами: внутреннее, прямое и внешнее. В работе приводится прямое соответствие, под которым я понимаю связь объектов 1 к 1 без внутреннего и внешнего контекста. Под внешним соответствием я понимаю функториальные свойства; им уделено мало внимания в данной работе, тем не менее, приведены все необходимые ссылки. За кадром и данной работы, и литературы, остаётся внутреннее соответствие, которое, тем не менее, самое интересное, т.к. оно обычно не включено в привычные отображения; понимается это мной следующим образом: отображения между объектами являются внутренними по отношению к функторам; например, функтор $\mathrm{Hom}(—, A)$ никак не затрагивает внутреннюю структуру A; биекция между множествами ничего не говорит о соответствии подмножеств соответствующих друг другу элементов. Именно с этим связан тот факт, что если центральная простая алгебра соответствует определённому многообразию Севери-Брауэра, то подалгебры могут не соответствовать подмногообразиям у данных объектов.

Возвращаясь к вопросу о том, кто будет читать эту работу; для кого она? Я исходил по большей части из того, что потенциальный читатель не в теме и, прочитав работу, может заинтересоваться ею; людям в теме данная работа может быть интересна для предоставления её людям не в теме и, возможно, стратегиями решения гипотезы Амицура. Иными словами, это *обзор с покрытием связанных тем в разной степени*. Этим обусловлено обилие ссылок на литературу, в которой можно найти предварительные сведения, подробные исторические справки, задачи и так далее.

Глава 2

Обзор предварительных сведений

2.1 Абелевы группы

Многие объекты, с которыми мы будем иметь дело, являются абелевыми группами. Нам понадобится информация о их классификации. А именно, абелевы группы бывают 3 видов:

1. **делимые**: группа D делима $\iff$ для $x \in D$ и $n \in \mathbb{N}$ существует такой $y \in D$, что $ny = x$;
2. **конечно порождённые**: группа G конечно порождена $\iff$ существует конечный набор элементов

$$g_1, \dots, g_n \in G$$

такой, что любой элемент x представляется в виде $x = k_1 g_1 + \dots + k_n g_n$, где $k_i \in \mathbb{Z}$;

3. все остальные.

Отметим, что одновременно делимой и конечно порождённой группой является только тривиальная группа.

Полезный факт 2.1.1. *Делимая группа является прямой суммой копий $\mathbb{Q}$ и $\mathbb{Z}(p^\infty)$ для простых (возможно, повторяющихся) p . [Fuc70, p. 104]*

Группа $\mathbb{Z}(p^\infty)$ может быть по-разному записана в виде

$$\mathbb{Z}\left[\frac{1}{p}\right] \Big/ \mathbb{Z} \cong \varinjlim_n \mathbb{Z}/p^n\mathbb{Z} \cong \varinjlim_n \mu_{p^n} \cong \mathbb{Q}_p/\mathbb{Z}_p \cong \langle g_1, g_2, \dots \mid g_1^p = 1, g_2^p = g_1, g_3^p = g_2, \dots \rangle,$$

что читается слева направо соответственно как: все не целые дроби с степенями p в знаменателе, копредел по $n = 1, 2, \dots$ циклических групп порядка p^n, копредел по $n = 1, 2, \dots$ групп корней из 1 степени p^n, фактор p-адических чисел по целым p-адическим числам, копредставление группы.

Полезный факт 2.1.2. *Конечно порождённая группа является прямой суммой циклических групп. [Gri70, p. 15]*

Иными словами, нет других конечно порождённых групп, кроме групп вида

$$G = \mathbb{Z}^a \oplus \mathbb{Z}/p_1^{k_1}\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_n^{k_n}\mathbb{Z},$$

где $a \in \mathbb{N}_0$, а p_i могут повторяться (как и их степени); нет также и никаких делимых групп, кроме

$$D = \bigoplus_{r_0(D)} \mathbb{Q} \oplus \bigoplus_p \left[\bigoplus_{r_p(D)} \mathbb{Z}(p^\infty) \right],$$

где $r_0(D)$ — torsion-free ранг группы, $r_p(D)$ — p-ранг группы, см. [Fuc70, p. 85]. Для конечно порождённой группы G выше, например, a является её torsion-free рангом, а p-рангом — количество слагаемых $\mathbb{Z}/p\mathbb{Z}$.

Элементы конечного порядка в группе G образуют подгруппу кручения, обозначаемую $\mathrm{Tor}(G)$; в свою очередь факторгруппа $G/\mathrm{Tor}(G)$ не содержит элементов конечного порядка, т.е. является группой, свободной от кручения. Например, в случае конечно порождённой группы G имеем:

$$\mathrm{Tor}(G) = \mathbb{Z}/p_1^{k_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{k_n}\mathbb{Z}$$

$$G/\mathrm{Tor}(G) = \mathbb{Z}^a$$

В данном случае $G = G/\mathrm{Tor}(G) \oplus \mathrm{Tor}(G)$, т.е. "отнять и прибавить" работает. Это верно и для делимых групп:

$$\mathrm{Tor}(D) = \bigoplus_p \left[\bigoplus_{r_p(D)} \mathbb{Z}(p^\infty) \right]$$

$$D/\mathrm{Tor}(D) = \bigoplus_{r_0(D)} \mathbb{Q}$$

$$D = D/\mathrm{Tor}(D) \oplus \mathrm{Tor}(D)$$

Полная классификация групп, отличных от конечно порождённых или делимых, на данный момент отсутствует, и для них "отнимание и прибавление" подгруппы кручения может давать группу, отличную от изначальной.

Оказывается, если пойти дальше и "отнять и прибавить" удачно выбранную подгруппу (не подгруппу кручения), проблемы наступают уже в случае конечных групп, а именно, если порядок группы равен 4, 8, 9, 12, 16, 18, ... , т.е. делится на степень простого числа, большую или равную 2. Например, если B — группа такого порядка, а A — подгруппа в B, то хочется ожидать, что $B = B/A \oplus A$. Это не всегда так:

$$\mathbb{Z}/4\mathbb{Z} \Big/ \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}, \text{ но } \mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/8\mathbb{Z} \Big/ \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z}, \text{ но } \mathbb{Z}/8\mathbb{Z} \ncong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

и т.д.

Этот эффект возникает потому, что существует больше одной группы каждого из порядков выше, а именно, если $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$, то существует $k_1 \cdot \ldots \cdot k_m$ различных групп порядка n; см. конкретный пример [BC68, с. 201, задача 6.49], и является наглядным примером проблемы **расширения групп**. Позже мы увидим, что эта проблема свойственна и для не абелевых групп.

Приведённая выше классификация нам необходима ради следующего наблюдения. Оказывается, что группы когомологий являются группами кручения; таким образом, посчитать группу когомологий в конечно порождённом и делимом случаях означает найти её запись в виде $\mathbb{Z}/p_1^{k_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{k_n}\mathbb{Z}$ или $\bigoplus_p \left[\bigoplus_{r_p} \mathbb{Z}(p^\infty) \right]$. Приведём важные для дальнейшего изложения примеры групп и их свойства.

Делимые группы:

1. $\mathbb{Q}$, как легко видеть по определению.
2. $\mathbb{Q}/\mathbb{Z}$ — так же видно из определения делимой группы, но можно воспользоваться и тем, что факторгруппа делимой группы является делимой.

$$\mathbb{Q}/\mathbb{Z} \cong \varinjlim_p \mathbb{Z}(p^\infty) \cong \varinjlim_p \mathbb{Q}_p/\mathbb{Z}_p$$

Полезный факт 2.1.3. *Следующие условия равносильны:*

1. *D — делимая группа,*
2. *D — инъективная группа (или: инъективный объект в категории абелевых групп; или: в категории $\mathbb{Z}$-модулей),*

3. *контравариантный функтор* $\mathrm{Hom}_{\mathbb{Z}}(—, D)$ *является точным.* [Lam99, p. 71], [Wei94, p. 33-40]

2-е условие означает, что если делимая группа вкладывается в другую группу (т.е. является её подгруппой), то она выделяется как прямое слагаемое. Значит, если A — делимая группа, то в короткой точной последовательности абелевых групп $0 \to A \to B \to C \to 0$ понятно, что $B = A \oplus C$.

Литература

- [BC68] — *эталон* учебной литературы, имеется много задач с решениями и необходимая базовая теория, начиная с основ;
- [Fuc70], [Gri70], [Kap65], [Sha72] — теория бесконечных абелевых групп, в том числе описано взаимодействие с аппаратом гомологической алгебры.

2.2 Модули над кольцами

Мы обсудим несколько формульных представлений модулей, их взаимосвязь и удобство использования в том или ином случае. Ключевое отличие от модулей над группами, которые рассмотрены далее, в том, что R является R-модулем, в то время как группа G является G-модулем только в тривиальном случае $G = 0$. Итак,

Полезный факт 2.2.1. *Следующие условия эквивалентны:*

1. M *— R-модуль в смысле классического определения, например, из* [МИ21, *с. 29*]
2. $R \otimes_R M \cong M$ *является наиболее удобной записью. Она просто отражает суть названия "модуль": если мы возьмём какое-то кольцо A, являющееся R-модулем, то $A \otimes_R M$ является A-модулем; из набора колец $A_1, \ldots, A_n$ получается кольцо $A_1 \otimes_{\mathbb{Z}} \ldots \otimes_{\mathbb{Z}} A_n$, которое является модулем над каждым из колец, или, иначе говоря, является $A_1 \otimes_{\mathbb{Z}} \ldots \otimes_{\mathbb{Z}} A_n$-модулем — опять же, каждое кольцо является модулем над собой.*
3. $\mathrm{Hom}(R, M) \underset{\text{R-mod}}{\cong} M$ *удобно*[1] *с точки зрения дуализации: просто разворачиваем стрелки и получаем* $\mathrm{Hom}(M, R)$*; когда R — поле, последняя запись есть не что иное как ковекторы (линейные функционалы).*
4. *Задан гомоморфизм колец* $\varphi\colon R \to \mathrm{End}(M) = \mathrm{Hom}(M, M)$

При этом: единственность R-модуля M для заданных R и M = универсальное свойство $\otimes$ (применительно к R и M) = единственность гомоморфизма колец $\varphi\colon R \to \mathrm{End}(M)$ (т.к. φ не тривиально: $\varphi(0) \neq \varphi(1)$)

Литература

- [Pie82] — подробный справочник, который можно считать базовым по излагаемой в данной работе теории;
- [Айз17], [Lam99], [МИ21] — можно найти как базовую теорию модулей и колец, так и более продвинутый материал.

2.3 Модули над группами

Модули над группами нас интересуют в контексте неабелевых когомологий. Так как модули над группой G (G-модули) образуют категорию, возникает вопрос, как для неё отличается описание функторов Hom и $\otimes$. Один из подходов очевиден, так как имеется следующая эквивалентность категорий:

$$\mathbb{Z}[G]\text{-модули} \cong G\text{-модули}.$$

Что позволяет задать необходимые функторы на G-модулях просто индуцировав их из категории $\mathbb{Z}[G]$-модулей. С другой стороны, хоть вполне понятно, как дать ad-hoc определение функтора Hom для категории G-модулей,

[1] Коудобно.

сразу неясно, имеется ли genuine аналог $\otimes$. Мы оставим этот вопрос открытым; отметим, что в контексте излагаемой теории имеет место именно ad-hoc задание неабелевых когомологий, т.е. индуцирование с помощью эквивалентности с $\mathbb{Z}[G]$-модулями не рассматривается и потому возникает другой вопрос: эквивалентно ли имеющееся ad-hoc задание подходу с индуцированием? — этот вопрос мы также опустим и займёмся изложением необходимой теории.

Определение 2.3.1. ***Проконечной группой*** *называется предел конечных групп.*

Мотивацией введения данного определения в нашей работе могут служить следующие **примеры проконечных групп:**

1. Любая конечная группа;
2. Абсолютная группа Галуа числового поля (т.е. конечного расширения $\mathbb{Q}$);
3. Аддитивная группа p-адических целых чисел.

Далее Γ — проконечная группа. Отметим, что на ней задаётся топология: на конечных группах рассматривается дискретная топология (и потому они компактны и Хаусдорфовы); значит, Γ — так как это предел Хаусдорфых и компактных пространств — так же Хаусдорфово и компактно. Описание данной топологии можно найти также в [ГШ18, с. 47]. Это допускает альтернативное определение проконечной группы, см., например, [Sha72, с. 7].

Определение 2.3.2. *Дискретное топологическое пространство X называется* Γ***-множеством*** $\iff$ Γ *непрерывно действует слева на X. Если X к тому же является группой, то X называется* Γ***-группой***. *И если X — абелева группа —* Γ***-модулем***.

Мы ввели эти 3 разных понятия для того, чтобы показать, чтобы сказать следующее: для Γ-множества A можно определить $H^0(\Gamma, A)$, для Γ-группы A — $H^0(\Gamma, A)$ и $H^1(\Gamma, A)$; и $H^i(\Gamma, A)$ для любого $i = 0, 1, \ldots$, если A — Γ-модуль.

Литература

- [ГШ18] — связанная теория изложена через последовательность упражнений;
- [Knu+98] — всеобъемлющая книга, базовая в излагаемой теории, как [Pie82], но с другим покрытием. Можно найти подробное описание связанных с проконечными группами объектов.

2.4 Точные последовательности. Резольвенты

Наиболее естественно точные последовательности возникают так, как показано в [Айз17, с. 595-597]. Мы же обсудим комплекс

$$\ldots \xrightarrow{\partial} \mathbb{Z}[G^{\times 2}] \xrightarrow{\partial} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

и покажем, что это проективная резольвента для G-модуля $\mathbb{Z}$, так, как это предлагается в упражнениях [ГШ18, с. 16-17]. По определению,

$$\mathbb{Z}[G^{\times i}] = \left\{ \sum n_{g_1 \ldots g_i} \cdot (g_1, \ldots, g_i) \mid n_{g_1 \ldots g_i} \in \mathbb{Z} \right\}$$

и

$$\partial \colon \mathbb{Z}[G^{\times (i+1)}] \to \mathbb{Z}[G^{\times i}],\ i \geq 0,$$

$$\partial(g_1, \ldots, g_{i+1}) = \sum_{j=1}^{i+1} (-1)^{j+1} (g_1, \ldots, \widehat{g_j}, \ldots, g_{i+1}),$$

где $\widehat{g_j}$ означает пропуск (буквально) элемента на позиции j. Из определения видно, что $G^{\times i} = \overbrace{G \times ... \times G}^{G \text{ встречается } i \text{ раз}}$ является базисом G-модуля $\mathbb{Z}[G^{\times i}]$[2], а потому он является свободным и, в частности, проективным объектом в категории G-модулей. Далее, ∂ действительно является морфизмом в категории G-модулей и выполнено $\partial \circ \partial = 0$, как видно из рутинной проверки:

$$\partial(g(g_1, ..., g_{i+1})) = \sum_{j=1}^{i+1}(-1)^{j+1}(gg_1, ..., \widehat{gg_j}, ..., gg_{i+1}) = g\left(\sum_{j=1}^{i+1}(-1)^{j+1}(g_1, ..., \widehat{g_j}, ..., g_{i+1})\right) = g\partial(g_1, ..., g_{i+1}),$$

$$\partial(g_1 + h_1, ..., g_{i+1} + h_{i+1}) = \sum_{j=1}^{i+1}(-1)^{j+1}(g_1 + h_1, ..., \widehat{g_j + h_j}, ..., g_{i+1} + h_{i+1}) =$$

$$= \sum_{j=1}^{i+1}(-1)^{j+1}\left((g_1, ..., \widehat{g_j}, ..., g_{i+1}) + (h_1, ..., \widehat{h_j}, ..., h_{i+1})\right) =$$

$$= \sum_{j=1}^{i+1}(-1)^{j+1}(g_1, ..., \widehat{g_j}, ..., g_i) + \sum_{j=1}^{i+1}(-1)^{j+1}(h_1, ..., \widehat{h_j}, ..., h_i) = \partial(g_1, ..., g_{i+1}) + \partial(h_1, ..., h_{i+1}),$$

$$(\partial \circ \partial)(g_1, ..., g_{i+1}) = \partial\Big((g_2, g_3, ..., g_{i+1}) - (g_1, g_3, g_4, ..., g_{i+1}) + (g_1, g_2, g_4, ..., g_{i+1}) -$$

$$-(g_1, g_2, g_3, g_5, ..., g_{i+1}) + ...\Big) = (g_2 + \varepsilon g_1, \chi g_2, g_4 + \varepsilon g_3, \chi g_4, ...),$$

где $\varepsilon = -1, \chi = 0$ если $i+1$ чётно, и $\varepsilon = 0, \chi = 1$, если нечётно. Тогда

$$i+1 \text{ нечётно} \implies \partial(g_2, g_2, g_4, g_4, ...) = (g_2 - g_2, 0, g_4 - g_4, 0, ...) = (0, ..., 0)$$

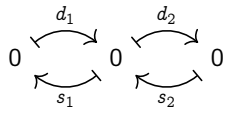
$$i+1 \text{ чётно} \implies \partial(g_2 - g_1, 0, g_4 - g_3, 0, ...) = (0, ..., 0)$$

Нам остаётся доказать точность комплекса, чтобы называть его проективной резольвентой. Для этого мы воспользуемся гомотопической эквивалентностью комплексов, но сначала объясним, как она работает. Рассмотрим некоторые объекты A, B, C и отображения $d_1 \colon A \to B$, $d_2 \colon B \to C$, при этом $d_2 \circ d_1 = 0$:

$$A \xrightarrow{d_1} B \xrightarrow{d_2} C$$

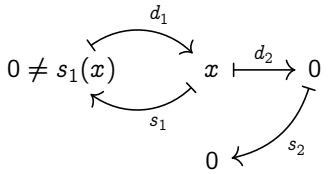
т.е. мы рассматриваем кусок комплекса, в котором нас интересуют гомологии в B. Гомология есть не что иное как цикл без границы, поэтому мы возьмём $x \in B$ и проанализируем его образ в C и прообраз в A; для этого обозначим $s_1 = d_1^{-1}$ и $s_2 = d_2^{-1}$ (смысл "обратимости" станет ясен далее). Тогда возможны следующие варианты:

1. **Тривиальный случай:**



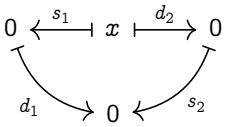
   Далее полагаем $x \neq 0$.

2. Цикл с границей, т.е. x переходит в 0 в C, но при этом имеет ненулевой прообраз в A:

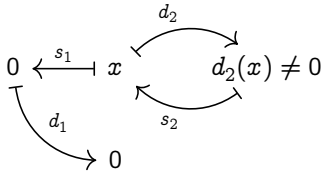


[2] В этом и заключается смысл определения $\mathbb{Z}[G^{\times i}]$: мы индексируем целые числа наборами $(g_1, ..., g_i)$ и рассматриваем их линейные комбинации.

3. **Цикл без границы, т.е. гомология**:



4. Не цикл; так как $d_2 \circ d_1 = 0$, то $s_1(x) = 0$:



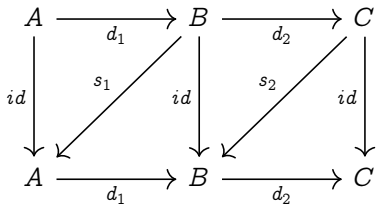
Мы замечаем, что **только** в 1 и 3 случаях отображения $d_1 s_1$ и $s_2 d_2$ дают 0 одновременно! Из данных диаграмм мы также видим, что это равносильно следующему:

$$(d_1 s_1 + s_2 d_2)(x) = 0 \iff x \text{ — гомология}$$

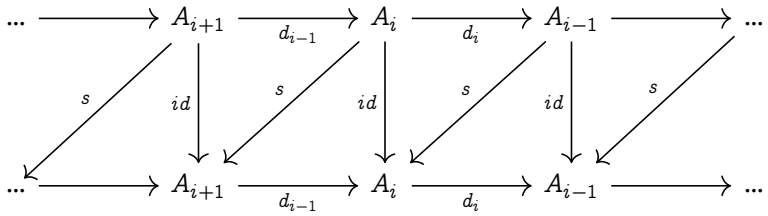
и, кроме того, $(d_1 s_1 + s_2 d_2)(x) = x$, если x — не гомология. Имеем:

$$d_1 s_1 + s_2 d_2 = id \iff \text{гомологий в } B \text{ нет}$$

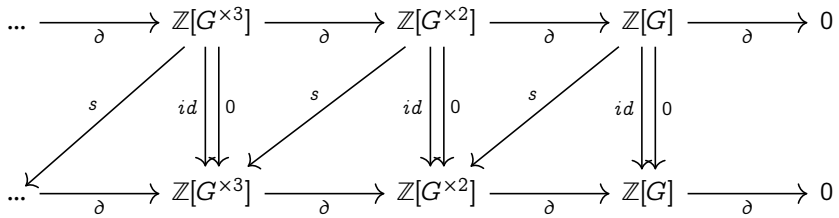
Для удобства мы запишем A, B, C и все имеющиеся стрелки в две строки и получим коммутативную диаграмму:



Так как мы рассматриваем комплексы, это превращается в



Обсудим дальнейшее обобщение. Нас интересует не столько сам комплекс, сколько его гомологии; в связи с этим 2 различных комплекса уместно идентифицировать в случае, если они имеют одинаковые гомологии. С такой позиции, например, точный комплекс не отличим от нулевого комплекса $\ldots \to 0 \to 0 \to 0 \to \ldots$, а в случае, как выше, говорят, что id гомотопно нулю. А именно, отображения f и g цепных комплексов называются гомотопными, если $f - g = \partial s + s\partial$ для некоторых s[3]. Мы воспользуемся этим для доказательства точности нашего комплекса:



[3] s может являться как одним и тем же отображением, заданным для разных членов комплекса, так и набором разных s_i.

где s задаётся как $s(g_1, ..., g_i) = (e, g_1, ..., g_i)$. Проверим, что $\partial s + s\partial = id - 0 = id$:

$$\partial s(g_1, ..., g_i) = \partial(e, g_1, ..., g_i) = (g_1, ..., g_i) + \sum_{j=1}^{i}(-1)^j(e, g_1, ..., \widehat{g_j}, ..., g_i) =$$

$$= (g_1, ..., g_i) + \sum_{j=1}^{i}(-1)^j s(g_1, ..., \widehat{g_j}, ..., g_i) = (g_1, ..., g_i) + s\left(\sum_{j=1}^{i}(-1)^j(g_1, ..., \widehat{g_j}, ..., g_i)\right) =$$

$$= (g_1, ..., g_i) - s\partial(g_1, ..., g_i)$$

Откуда из начала и конца цепочки равенств имеем

$$\partial s(g_1, ..., g_i) + s\partial(g_1, ..., g_i) = (g_1, ..., g_i)$$

Т.е.

$$\partial s + s\partial = id$$

Итак, мы построили проективную резольвенту для $\mathbb{Z}$.

Отметим, что простейший пример резольвент — короткие точные последовательности.

Литература

Так как это базовые объекты гомологической алгебры, то соответствующую теорию можно найти, например, в [Wei94], [Rot08].

Особую роль в гомологической алгебре занимают, как известно, спектральные последовательности; данная машинерия позволяет считать гомологии и когомологии, и в нашем случае с их помощью могут быть доказаны многие факты касательно группы Брауэра, см. [NSW20]. Любопытно также, что с помощью спектральных последовательностей можно просто доказывать базовые факты, например, лемму о змее, 5-лемму, см. [Vak17, с. 62—63]. Помимо хорошего введения [Cho06] отметим деталь, нигде не указываемую: уровни пишутся диагонально для удобной индексации (как и total complex; про total complex также отметим, что он возникает из представления элементов последовательности в виде градуирования); действительно, комплексы (резольвенты, точные последовательности) мы пишем горизонтально и естественно было бы ожидать вертикальную запись фильтрации или градуирования.

2.5 Функторы: тензорное произведение, функтор точек, Tor, Ext

Дадим кратку сводку интересующих нас функторов. A — некоторый R-модуль. Мы хотим вкратце показать, как формируются группы гомологий и когомологий в случае абелевой категории на примере R-mod.

Hom и $\otimes$

Функтор	Вариантность	Сопряжённость	Точность	Точен с другой стороны, если …
$— \otimes A$	ко	левый	справа	A плоский
$A \otimes —$	ко	левый	справа	A плоский
$\mathrm{Hom}(—, A)$	контра	правый	слева	A инъективен
$\mathrm{Hom}(A, —)$	ко	правый	слева	A проективен

Один из функторов, играющий ключевую роль в нашей работе, является контравариантным — $\mathrm{Hom}(—, A)$. Обсудим его сопряжённость и возникающий нюанс.

Теорема 2.5.1. *Для любого R-модуля N функтор* $\mathrm{Hom}(—, N)$ *является сопряжённым справа к самому себе.*

Производные функторы

Функтор	Вариантность	Производность
$\mathrm{Tor}_i^R(—, A)$	ко	левый производный
$\mathrm{Tor}_i^R(A, —)$	ко	левый производный
$\mathrm{Ext}^i_R(—, A)$	контра	правый производный
$\mathrm{Ext}^i_R(A, —)$	ко	правый производный

Доказательство. [Alu09, с. 536]. Замечание: $\mathrm{Hom}(—, N)$ **не является** сопряжённым слева к самому себе. Q. E. D.

Нюанс в том, что контравариантный $\mathrm{Hom}(—, N)$ стоит понимать как ковариантный $\mathrm{Hom}(—, N)$ из категории, двойственной к R-mod — $\text{R-mod}^{\mathrm{op}}$; т.к. предел в $\text{R-mod}^{\mathrm{op}}$ — копредел в R-mod, то теорема о сопряжённых функторах и пределах, которую мы приведём далее, говорит, что $\mathrm{Hom}(—, N)$ сохраняет пределы в $\text{R-mod}^{\mathrm{op}}$, т.е. сохраняет копределы в R-mod. Существенность данного замечания в том, что *пределы* в R-mod $\mathrm{Hom}(—, N)$, вообще говоря, не сохраняет.

Так как группы гомологий и когомологий являются объектами-инвариантами в том смысле, что по двум заданным объектам-аргументам мы получаем один объект (как обычно, с точностью до изоморфизма), при его поэтапном построении важно, чтобы промежуточно возникающие объекты были единственными с точностью, подходящей для единственности финальной конструкции. Алгоритм следующий:

1. Имеется некоторый R-модуль A; мы хотим посчитать гомологии с коэффициентами в R-модуле B. Первое действие — удобно записываем A в виде комплекса, concentrated in degree zero. Это означает, что мы теперь работаем в категории комплексов из объектов из R-mod и что все члены комплекса кроме нулевой позиции нулевые:

$$\begin{array}{ccccccccccc} \ldots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & A & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \ldots \\ \ldots & & n=2 & & n=1 & & n=0 & & n=-1 & & n=-2 & & \ldots \end{array}$$

2. Строим проективную резольвенту как морфизм комплексов, который есть не что иное как отображение аугментации ε:

$$\begin{array}{ccccccccccccc} \ldots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \ldots \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \varepsilon} & & \downarrow & & \downarrow & & \\ \ldots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & A & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \ldots \\ \ldots & & n=2 & & n=1 & & n=0 & & n=-1 & & n=-2 & & \ldots \end{array}$$

На этом этапе мы задаёмся вопросами: существует ли резольвента? Если их несколько, то как это повлияет на единственность группы гомологий? Ответами являются следующие теоремы:

Теорема 2.5.2. *Каждый R-модуль обладает проективной резольвентой.*

Доказательство. [Wei94, с. 34] Q. E. D.

Теорема 2.5.3 (О сравнении). *$\varepsilon\colon P_\bullet \to M$ — проективная резольвента для M, $f'\colon M \to N$ — морфизм в соответствующей категории. Тогда для любой резольвенты $\eta\colon Q_\bullet \to N$ для N существует отображение $f\colon P_\bullet \to Q_\bullet$ такое,*

что $\eta \circ f_0 = f' \circ \varepsilon$ *и* f *единственно с точностью до гомотопии комплексов.*

$$\begin{array}{ccccccccc} \dots & \longrightarrow & P_1 & \longrightarrow & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f'} & & \\ \dots & \longrightarrow & Q_1 & \longrightarrow & Q_0 & \xrightarrow{\eta} & N & \longrightarrow & 0 \end{array}$$

Доказательство. [Wei94, с. 36] Q. E. D.

Как обсуждалось ранее, у гомотопных комплексов совпадают гомологии, поэтому положив $M = N$ в последней теореме мы получаем ответ на вопрос о единственности группы гомологий. См. также [Wei94, с. 44].

3. Применяем функтор $- \otimes_R B$ (или $B \otimes_R -$, роли не играет; в силу ковариантности сохраняются направления стрелок):

$$\begin{array}{ccccccccccccc} \dots & \longrightarrow & P_2 \otimes_R B & \longrightarrow & P_1 \otimes_R B & \longrightarrow & P_0 \otimes_R B & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \dots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \dots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & A \otimes_R B & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \dots \end{array}$$

$$\begin{array}{ccccccc} \dots & n=2 & n=1 & n=0 & n=-1 & n=-2 & \dots \end{array}$$

На этом этапе отметим преимущество использования "полной" записи в виде морфизма комплексов: так проще увидеть, почему $L_0(F(A)) = F(A)$ $\big($и $R^0(F(A)) = F(A)\big)$:

$$L_0(F(A)) := \mathrm{H}_0(F(P_\bullet)) = \ker(F(P_0) \to 0)/\mathrm{im}(F(P_1) \to F(P_0)) = F(P_0)/\mathrm{im}(F(P_1)) = F(A),$$

что в нашей ситуации переводится как $\mathrm{H}_0(A, B) = A \otimes_R B$. В силу универсального свойства $\otimes$ единственность в смысле, указанном выше, сохраняется.

4. Считаем гомологии комплекса в верхней строке, просто по определению как фактор циклов по границам; получаем:

$$\begin{array}{ccccccccccccc} \dots & \longrightarrow & H_2(A,B) & \longrightarrow & H_1(A,B) & \longrightarrow & H_0(A,B) & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \dots \\ & & n=2 & & n=1 & & n=0 & & n=-1 & & n=-2 & & \end{array}$$

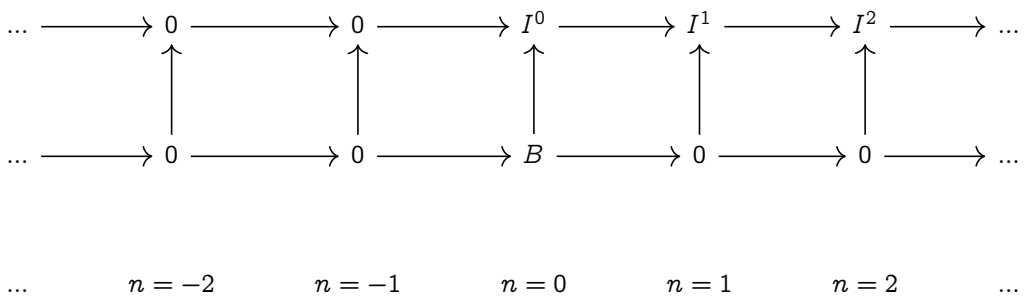
Аналогично получаются когомологии $\mathrm{H}^i(A, B)$:

1. Представляем B как комплекс, concentrated in degree zero. Отличие в направлении стрелок — мы поменяли индексы.

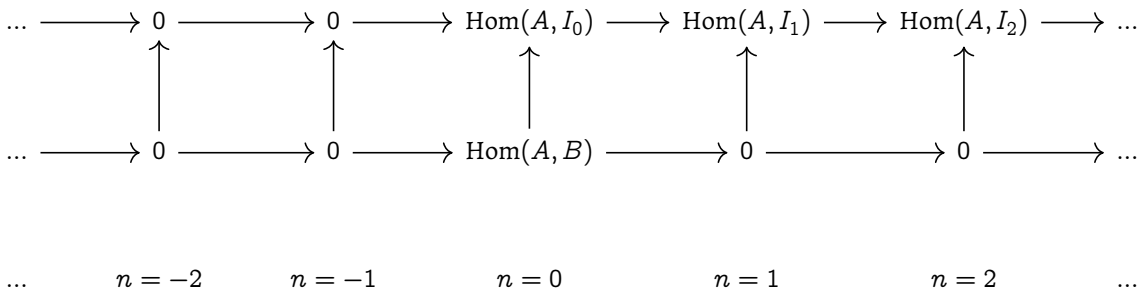
$$\begin{array}{ccccccccccccc} \dots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & B & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \dots \\ \dots & & n=-2 & & n=-1 & & n=0 & & n=1 & & n=2 & & \dots \end{array}$$

2. Строим инъективную резольвенту. Для неё верны аналогичные результаты о существовании и сравнении

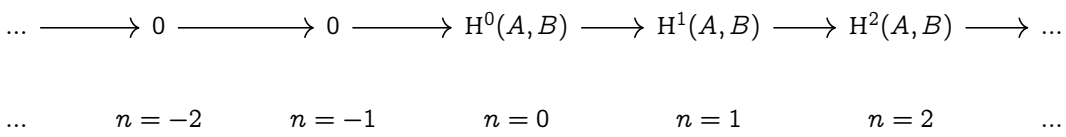
[Wei94, с. 40].



3. Далее применяем ковариантный $\mathrm{Hom}(A,—)$, получаем



4. Из комплекса в верхней строке имеем



   И так же $\mathrm{H}^0(A,B) = \mathrm{Hom}(A,B)$.

Отличие гомологий и когомологий при определении через левые и правые производные функторы соответственно в том, что для гомологий в любом случае необходима проективная резольвента либо по первому, либо по второму аргументу, т.к. $\otimes$ ковариантен по обоим из них; при подсчёте когомологий "начиная с A" необходимо использовать проективную резольвенту, т.к. $\mathrm{Hom}(—,B)$ контравариантен.

Формально это выражается следующими утверждениями:

Теорема 2.5.4.

$$\mathrm{Tor}_n^R(A,B) = L_n(A\otimes_R —)(B) \cong L_n(—\otimes_R B)(A)$$

Доказательство. [Wei94, с. 58] Q. E. D.

Теорема 2.5.5.

$$\mathrm{Ext}_R^n(A,B) = R^n\mathrm{Hom}(A,—)(B) \cong R^n\mathrm{Hom}(—,B)(A)$$

Доказательство. [Wei94, с. 63] Q. E. D.

Далее обсудим следующую важнейшую теорему.

Теорема 2.5.6 (**О сопряжённых функторах и пределах**). *$L\colon A\to B$ — функтор, сопряжённый слева к $R\colon B\to A$. Тогда:*

1. *L сохраняет все копределы;*
2. *R сохраняет все пределы.*

Доказательство. https://ncatlab.org/nlab/show/adjoint+functor+theorem. Отметим также, что в случае контравариантного функтора предел переходит в копредел и наоборот, см. [Rot08, с. 239—240] для формального определения сохранения. Q. E. D.

Другими словами, сопряжённые слева функторы коммутируют с копределами; двойственно, сопряжённые справа функторы коммутируют с пределами.

Простейший пример, иллюстрирующий сказанное — $(A \oplus B) \otimes C \cong (A \otimes C) \oplus (B \otimes C)$ — "коммутирование $\oplus$ и $\otimes$" (или, проще говоря, дистрибутивность); сопряжённый слева функтор — $\otimes$; $\oplus$ — копроизведение (пример копредела). Приведём частные случаи данной теоремы, непосредственно относящиеся к нашему контексту.

Теорема 2.5.7. *В* R-mod *выполняется:*

1. $A \otimes_R \lim B_i \cong \lim (A \otimes_R B_i)$;
2. $\mathrm{Hom}(A, \lim M_i) \cong \lim \mathrm{Hom}(A, M_i)$;
3. $\mathrm{Hom}(\mathrm{colim}\, M_i, B) \cong \lim \mathrm{Hom}(M_i, B)$.

Доказательство. [Rot08, с. 241], [Rot08, с. 236], [Rot08, с. 240] Q. E. D.

Так как многие объекты, встречающиеся на месте первого или второго аргументов при подсчёте гомологий (когомологий), являются тем или иным пределом или копределом, мы, пользуясь утверждением выше, можем разбить вычисление гомологий (когомологий) от сложного, т.е. сложенного как предел или копредел, объекта на части, и затем взять предел/копредел.

В контексте нашей работы рассматривается группа Брауэра, для подсчёта которой применяется $\mathrm{Hom}(—, B)$ к проконечной группе, которая по определению является пределом, — но $\mathrm{Hom}(—, B)$, вообще говоря, с пределами не коммутирует, как обсуждалось выше, — в этом и состоит интерес изучаемого объекта. Тем не менее, имеются следующие полезные результаты:

Теорема 2.5.8.

$$\mathrm{Ext}^n_R\left(\bigoplus_{k\in K} A_k, B\right) \cong \prod_{k\in K} \mathrm{Ext}^n_R(A_k, B)$$

Доказательство. [Rot08, с. 418] Q. E. D.

и

Теорема 2.5.9.

$$\mathrm{Ext}^n_R\left(A, \prod_{k\in K} B_k\right) \cong \prod_{k\in K} \mathrm{Ext}^n_R(A, B_k)$$

Доказательство. [Rot08, с. 419] Q. E. D.

Литература

Помимо упомянутых в предыдущем параграфе, [Alu09].

2.6 Категории и эквивалентности

Вкратце отметим, что смысл категории в том, что это удобная, например, для классификации совокупность объектов одной природы; эквивалентности между категориями стоит понимать примерно так же, как понимается изоморфность алгебраических объектов: отождествление "с точностью до" и отсутствие информации об отождествлении "подобъектов" : как изоморфизм групп ничего не говорит об внутреннем сопоставлении подмножеств сопоставленных элементов группы, так и функторы не говорят о сопоставлении элементов объектов. В

этом смысле категории "на уровень выше" множеств. Место изоморфизма групп (сохраняющего структуру группы) занимает пара из функтора и обратного к нему, композиции в обоих порядках которых натурально изоморфны тождественным функторам из соответствующих категорий — как видно, всё то же общее понятие сохранения структуры.

Так как в данной работе мы сталкиваемся с вопросом классификации объектов, уместно сказать, что это за объекты, т.е. какие категории вовлечены, и является ли объект чем-то знакомым и, возможно, уже классифицированным, — в этом помогают эквивалентности категорий.

- R-mod — категория R-модулей (R — коммутативное кольцо с 1);
- G-mod — категория G-модулей (G — проконечная группа);
- $\mathbb{Z}[G]$-mod — категория $\mathbb{Z}[G]$-модулей;
- Set_G — категория G-множеств;
- BS_{n-1}^{K} — категория многообразий Севери-Брауэра размерности $n-1$ над полем K, морфизмы в которой — изоморфизмы схем над K;
- $\mathrm{BS}_{n-1}^{/K}$ — категория многообразий Севери-Брауэра размерности $n-1$ над любым расширением поля K, морфизмы — композиция изоморфизма схем над K с $\mathrm{id} \times \mathrm{Spec}\, a \colon X \times_{\mathrm{Spec}\, L} \mathrm{Spec}\, L' \to X$, где $a \colon L \to L'$ — гомоморфизм полей, содержащих K;
- Az_n^K — категория центральных простых алгебр над K размерности n^2; морфизмы — изоморфизмы K-алгебр, сохраняющие единицу (отметим, что обозначение Az используется потому, что обобщением центральных простых алгебр являются алгебры Адзумаи);
- $\mathrm{Az}_n^{/K}$ — категория центральных простых алгебр размерности n^2 над любыми расширениями поля K; морфизмы — гомоморфизмы K-алгебр, сохраняющие единицу;
- $\mathrm{Mat}_n^{L/K}$ — категория расщепляющихся (поэтому Mat) центральных простых алгебр размерности n^2 над L; морфизмы — σ-линейные изоморфизмы, сохраняющие единицу, $\sigma \in \mathrm{Gal}(L/K)$;
- $\mathrm{Sch}^{L/K}$ — L-схемы;
- $\mathrm{P}_{n-1}^{L/K}$ — подкатегория в $\mathrm{Sch}^{L/K}$, состоящая из L-схем, изоморфных P_L^{n-1}; морфизмы — изоморфизмы.

Некоторые эквивалентности:

- G-mod $\cong \mathbb{Z}[G]$-mod;
- $\mathrm{Mat}_n^{L/K} \cong \mathrm{P}_{n-1}^{L/K}$, см. [Jah03, с. 37]. Они также антиэквивалентны, см. [Jah03, с. 38];
- $\mathrm{Az}_n^{/K} \cong (\mathrm{BS}_{n-1}^{/K})^{\mathrm{op}}$. В частности, $\mathrm{Az}_n^{L} \cong (\mathrm{BS}_{n-1}^{L})^{\mathrm{op}}$ для каждого расширения L/K, см. [Jah03, с. 39];
- $\mathrm{Az}_n^{K} \cong \mathrm{BS}_{n-1}^{K}$, см. [Jah03, с. 43].

См. также [Jah03, с. 7].

Литература

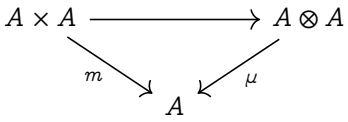
Для понимания теории категорий имеется исключительная по качеству книга [LS09], эталон учебной литературы. В остальном теория категорий в чистом виде в контексте данной работы не рассматривается, и потому необходимая часть покрывается книгами по гомологической алгебре, указанными выше.

2.7 Алгебры над кольцами

Алгебра над кольцом получается из модуля над кольцом одним из двух равносильных способов:

1. Добавление билинейного отображения $m\colon A \times A \to A$;
2. Добавление линейного отображения $\mu\colon A \otimes A \to A$.

Равносильность/эквивалентность выражается, как обычно, с помощью коммутативной диаграммы:



Отметим порядок происходящего: имея m, мы, постулировав, что диаграмма коммутирует, определяем μ индуцированием (верхняя стрелка определена по теореме о существовании $\otimes$ для любых двух модулей); обратно, имея μ, мы из коммутирования диаграммы индуцированием получаем m. Данная конструкция приведена для того, чтобы подчеркнуть её неявное присутствие в манипуляциях с $\otimes$. См., например, [Pie82, с. 179].

Литература

Подойдут [Pie82] и другие, указанные выше, для модулей над кольцами.

2.8 Классическая теория Галуа. Когомологии Галуа

Определение 2.8.1. ***Абсолютной группой Галуа*** *поля K называется, эквивалентно, любой из следующих объектов:*

1. *Группа Галуа расширения K^{sep}/K, где K^{sep} — сепарабельное замыкание поля K;*
2. *Предел по всем группам Галуа конечных расширений поля K.*

Существование и единственность абсолютной группы Галуа в первом варианте определения гарантируется следующим результатом.

Теорема 2.8.1.

1. *Каждое поле обладает сепарабельным замыканием;*
2. *Любые два сепарабельных замыкания поля изоморфны.*

Доказательство. [Mil22, с. 117] Q. E. D.

Из второго определения видно, что абсолютная группа Галуа является проконечной группой. Любопытно, что верен обратный, в некотором смысле, результат:

Теорема 2.8.2 (Тэйт). *Каждая проконечная группа G является группой Галуа некоторого расширения Галуа.*

Доказательство. [Mil22, с. 132]. Отметим, что в доказательстве дано и построение такого расширения, которое, к тому же, является не единственным. Q. E. D.

Далее приведём ответ на важный вопрос: почему скрещенный гомоморфизм выглядит так, как он выглядит: $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$ (или же: $f(\sigma\tau) = f(\sigma) \cdot \sigma f(\tau)$). Для объяснения необходимо прочитать [Mil22, с. 91] в обратном порядке: мы рассматриваем циклическую группу Галуа G порядка n, порождённую σ, и хотим иметь взаимно однозначное соответствие: отображение $(f\colon G \to M) \leftrightarrow x \in M$, где M — G-модуль, а x — решение уравнения $x + \sigma x + \ldots + \sigma^{n-1}x = 0$[4]. То есть наша цель, другими словами, чтобы отображение, которое мы

[4] Точнее, x обозначает в одном случае решение, а в другом — переменную.

назовём скрещенным гомоморфизмом, определялось своим значением в порождающем элементе, и наоборот; с учётом уравнения выше. Для этого мы естественно полагаем $f(\sigma) = x$, тогда уравнение принимает вид

$$f(\sigma^n) = f(\sigma) + \sigma f(\sigma) + \ldots + \sigma^{n-1} f(\sigma) = 0.$$

Действительно, естественно ожидать, что отмеченная точка в $0 \in M$ соответствует значению f в отмеченной точке $\sigma^n = 1$, т.е. $f(1) = 0$. Далее естественно полагать, что значения f для σ^{n-1}, σ^{n-2}, … выглядят так:

$$f(\sigma^{n-1}) = f(\sigma) + \sigma f(\sigma) + \ldots + \sigma^{n-2} f(\sigma),$$

$$\ldots$$

$$f(\sigma^3) = f(\sigma) + \sigma f(\sigma) + \sigma^2 f(\sigma),$$

$$f(\sigma^2) = f(\sigma) + \sigma f(\sigma),$$

откуда ясно, что естественно назвать скрещенным гомоморфизмом $f\colon G \to M$ такое, что

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau).$$

Причиной же желания построения соответствия $f \leftrightarrow f(\sigma)$ является аналогия с $\mathrm{Hom}(R, M) \cong M$, где M — R-модуль.

Далее: как могут выглядеть скрещенные гомоморфизмы? Один из вариантов —

$$f(\sigma) = x - \sigma x,$$

или, так как это выполнено для любого $x \in M$,

$$f(\sigma) = -x + \sigma x.$$

В мультипликативной записи:

$$f(\sigma) = x^{-1} \cdot \sigma x.$$

Такой скрещенный гомоморфизм называется **главным**. В некотором смысле, как коммутатор показывает степень неабелевости, так главный скрещенный гомоморфизм показывает, насколько нетривиально действует G на M; в этом мотивация его рассмотрения. Отметим, что если M — тривиальный G-модуль, т.е. если $\sigma m = m$ для всех $\sigma \in G$ и $m \in M$, то скрещенный гомоморфизм является обычным гомоморфизмом, а главный скрещенный гомоморфизм тривиален, т.е. $f(\sigma) = 0$, как видно из формул выше.

Литература

Изложение классической теории Галуа с исторической справкой может быть найдено в [Ste03]. См. также [Mil22]. Теория когомологий Галуа может быть найдена в [Knu+98], [NSW20], [SC21].

2.9 Универсальное свойство и переписывание

Цель данного параграфа — обсудить понятие универсального свойства, динамику и метаморфозы объектов и ответить на вопрос: что значит быть равными? Мы обсудим следующие тезисы:

1. Универсальное свойство = единственность определяемого объекта
2. $=$ и $\cong$ — одно и то же[5].

[5] Данное рассуждение носит концептуальный характер и отражает видение автора; высказанные идеи, как позже оказалось, находят отражение в HoTT (Homotopy Type Theory) в той или иной степени; авторское утверждение о том, что $=$ и $\cong$ — одно и то же (в определённой степени), сформулировано как аксиома Воеводского, которая является краеугольным камнем HoTT. Такие вещи, как переписывание/вычисление, также оказываются сформулированными понятиями (λ-абстракция, β-правило, η-правило, …). См. [13] и [Rij22]

3. Универсальное свойство — подозрение на функтор

Ядро, прямая сумма, тензорное произведение[6] — объекты, имеющие и классические определения, на объемлющем языке которых они являются единственными (у отображения единственное ядро, прямая сумма двух, например, групп единственна, тензорное произведение модулей единственно), так и определения на категорном языке, где они определяются как общая конструкция, совпадающая с классическими определениями в привычных случаях, например, в категории модулей над кольцом; на основании этого в определении таких объектов говорится, что они обладают универсальным свойством (= единственность на категорном языке). Общность конструкции заключается в том, что конкретная категория не называется, и поэтому существование ядер, прямых сумм, тензорных произведений и их универсальное свойство необходимо проверять в конкретно выбранной категории — это позволяет расширить область применимости данных понятий.

В то же время группа, кольцо, поле — примеры шаблонов, под которые попадает больше одного объекта. Такие понятия не обладают универсальным свойством.

Ключевой концепцией тут является **переписывание**. Рассмотрим пример натуральных чисел в аксиоматике Пеано:

1. $1 \in \mathbb{N}$
2. $x \in \mathbb{N} \implies S(x) \in \mathbb{N}$
3. ...

где S означает функцию, дающую следующий элемент. Итак, наши натуральные числа выглядят так:

$$1,\ S(1),\ S(S(1)),\ S(S(S(1)),\ \ldots$$

Мы сразу видим, что даже для небольших чисел количество места, которое занимают "S больше, чем нам хотелось бы. Так что мы вводим знак "2"и говорим: "отныне 2 будет означать $S(1)$ т.е. $2 = S(1)$. Теперь мы можем сказать "натуральные числа"вот так:

$$1,\ 2,\ S(S(1)),\ S(S(S(1)),\ \ldots$$

или так:

$$1,\ 2,\ S(2),\ S(S(2)),\ \ldots$$

Ситуация улучшилась, но у нас всё ещё есть $S(2)$, $S(S(2))$, $S(S(S(2)))$ и другие числа, которые мы хотим писать короче. Аналогично мы вводим "3", "4", ... и так как наша фантазия и (или) память ограничена, а натуральные числа бесконечны, мы перестаём придумывать новые знаки и приходим к, например, известной десятичной системе исчисления. Таким образом, из

$$1,\ S(1),\ S(S(1)),\ S(S(S(1)),\ \ldots$$

мы получили

$$1,\ 2,\ 3,\ 4,\ \ldots$$

и сохранили место на бумаге/экране, убрав S. К тому же, введение десятичной системы сделало наше обращение с натуральными числами **удобнее**. Это пример **переписывания**. Можно изобразить этот процесс следующим образом:

$$1,\ S(1),\ S(S(S(1))),\ \ldots \qquad \rightsquigarrow \qquad 1,\ 2,\ 3,\ \ldots$$

[6] В подходящей категории

Но что если мы развернём ситуацию? Представим, что мы имеем $1,\ 2,\ 3,\ \ldots$. По какой-то причине мы хотим получить эту странную нотацию с "S". Ясно, что рассуждение выше работает и в обратную сторону и мы можем изобразить переписывание в обратную сторону как:

$$1,\ 2,\ 3,\ \ldots \qquad \rightsquigarrow \qquad 1,\ S(1),\ S(S(S(1))),\ \ldots$$

Единственная разница заключается в том, что мы взяли некоторые свойства из немой части контекста и сказали их, т.е. мы ввели аксиомы. Другими словами, сделали неявное явным. Ясно также, что можно переписать используя и любые другие обозначения:

$$1 \rightsquigarrow a$$

$$2 \rightsquigarrow b$$

$$\ldots$$

или, напротив, мы могли бы начать с a, подразумевая "один b, подразумевая "два"и так далее. Суть такова: *объект не зависит от того как мы его записываем.* Вот несколько эквивалентных формулировок:

1. Объект инвариантен относительно того, как мы его обозначаем, т.е. неважно, как мы его запишем, — он останется неизменным.

2. Мы можем производить вычисления: вычисление есть не что иное как переписывание в более удобном виде; например, переписывание $2+2$ как 4, переписывание групп в виде $\mathbb{Z}$ и факторов, и т.д. Вообще говоря, смысл вычисления (= переписывания) в том, чтобы получить более удобное формульное представление. В частности, $\sqrt{2}$ уже вычислен (тавтологично) для некоторых людей, в то время как для других вычислением может быть его переписывание в виде $1.4142\ldots$. Смотря как посмотреть!

Мы идём дальше и обозначим переписывание какого-то A в B как $x : A \rightsquigarrow B$. Но мы знаем много других букв, знаков и символов, поэтому могли бы записать переписывание и в виде $y : A \rightsquigarrow B$. Абсолютно ясно, что x и y делают одно и то же: говорят нам, что A и B переписываются друг в друга и означают одно и то же, или, иначе говоря, они обозначают один и тот же объект! Так что мы можем переписать переписывания друг в друга, скажем, z — переписывание x в y, т.е. $z : x \rightsquigarrow y$. Ясно, что можно продолжать этот процесс до бесконечности: переписывать переписывания переписываний и т.д.

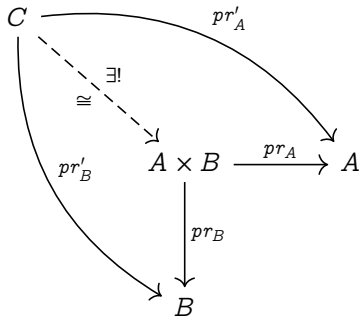
Это *в точности* то, что говорит **универсальное свойство**. Рассмотрим подробно пример произведения в категорном смысле: для объектов A и B существует объект, *обозначаемый* $A \times B$ вместе с соответствующими морфизмами (отображениями) $A \times B \to A$ и $A \times B \to B$. Рисуется следующая диаграмма:

$$\begin{array}{ccc} A \times B & \longrightarrow & A \\ \downarrow & & \\ B & & \end{array}$$

Можно задаться вопросом: сказали ли мы только что, что конструкция зависит от A, B и $A \times B$, то есть, что только этими буквами можно обозначать определяемый объект? Очевидно, нет. Всегда было ясно из контекста, что различные определения одного и того же могут использовать разные обозначения; порой обозначения одного и того же могут отличаться настолько, что переписывание одного в другое превращается в "критерий "эквивалентное определение а порой и вовсе в нерешаемые задачи классификации.

Наша цель — уменьшить немую часть контекста, сделать неявное явным, и для этого на примере произведения мы уточним его определение. Рассмотрим 2 подхода:

1. Мы говорим, что если есть какой-то объект, обозначаемый C, *такой же*, как и $A \times B$, с морфизмами $C \to A$ и $C \to B$, которые *такие же*, как и $A \times B \to A$ и $A \times B \to B$ соответственно, то это одно и то же произведение; рисуем следующую диаграмму



и говорим: "она коммутирует". Объясним происходящее.

"$A \times B \to A$ — одно и то же с $C \to A$"означает, что есть *какой-то* морфизм и мы знаем два его имени (два явления, две ссылки, два представления и т.д.); обозначим его как $pr_A : A \times B \to A$ и $pr'_A : C \to A$. Так как мы рассматриваем один морфизм, можно заключить, что C и $A \times B$ обозначают один и тот же объект. Но что если бы pr_B и pr'_B обозначали два разных морфизма? Тогда, как минимум, мы не могли бы идентифицировать одно произведение с другим; могло бы оказаться и так, что C и $A \times B$ означали бы разные объекты; но это не наш случай.

Разберём диаграмму.

Пунктирная стрелка $\dashrightarrow$ означает, что есть морфизм, но "он не задан"; ясно, что это пример переписывания, обозначаемый $\cong$ и называемый *изоморфизмом*. Знак $\exists!$ подчёркивает, что этот морфизм вписывается в нашу концепцию переписывания, т.е. что мы не имели ничего сверх сказанного; это *знак*, а не **символ**. Кроме того, $\exists!$ обычно читается как "единственный что само собой понимается как "единственный с точностью до единственного изоморфизма или как "единственный с точностью до единственного изоморфизма, который единственен с точностью до единственного изоморфизма"и так далее (переписывание переписываний ...).

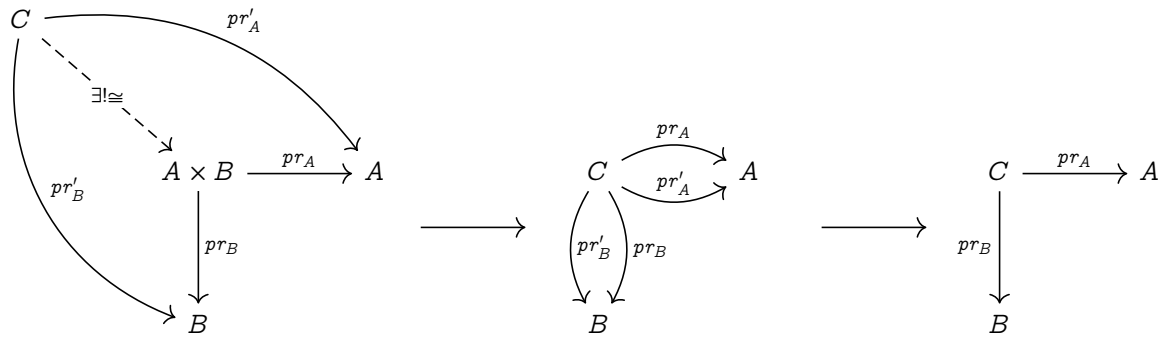
Хорошо, но что же означает "диаграмма коммутирует"? Обычно под $\to$ мы подразумеваем, что мы трансформируем один объект в другой внутренне, т.е. как отображение множеств. С такой позиции любая стрелка $\to$ может быть представлена как коллекция стрелок $\mapsto$. Стоит отметить, что $\mapsto$ в хорошей ситуации является изоморфизмом[7] (переписыванием), т.к. он соединяет *точки*, т.е. некоторые сущности, внутренняя структура которых в данном контексте нас не интересует[8]

Сконцентрируемся на $A \times B, C, A$ и отображениях между ними. Так как $A \times B$ и C — один объект, выберем в нём точку, дав ей имя, скажем x, и посмотрим, куда она пойдёт по стрелкам $\mapsto$ из pr_A и pr'_A. Но pr_A и pr'_A — одно и то же, т.е. это одно отображение, поэтому мы получаем следующую картинку:

[7]Можно задаться вопросом: что если две точки отображаются в одну? Как определить обратный путь? Ответ таков, что, например, в категории R-модулей этот случай соответствует проекции/факторизации, поэтому в качестве прообраза мы можем выбрать "канонического"представителя класса эквивалентности.

[8]Действительно, несмотря на множества множеств и подобные вещи, в контексте момента мы всегда имеем дело с 2-уровневой иерархией вида "множество-точки". Возможно, кому-то более комфортно воспринимать $\mapsto$ как изоморфизм тривиальных групп или иную идентификацию тривильных структур (которые в данном контексте рассматриваются как точки).

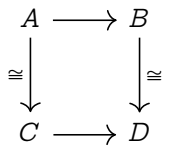
Такой треугольник называется *коммутирующим*.[9] Когда все треугольники, квадраты и т.д. в диаграмме коммутируют, то мы говорим, что и сама диаграмма коммутирует. Формально, если мы обозначим $C \to A \times B$ как f, то смысл правой картинки может быть передан и записью $pr'_A = pr_A \circ f$. Так как f — наше переписывание, приравнивание имён, то ясно, что его можно переписать как id, т.е. $\dashrightarrow$ пропадает/стягивается. Формально, композиция выше превращается в $pr'_A = pr_A$. Те же рассуждения применяются и к B вместе с стрелками к нему, и мы получаем ещё один коммутирующий треугольник и $pr_B = pr'_B$. В конце концов мы избавляемся и от pr'_A и pr'_B, т.к. они не несут новой информации (ведь они есть то же самое что и pr_A и pr_B соответственно). Изображение нашей процедуры:



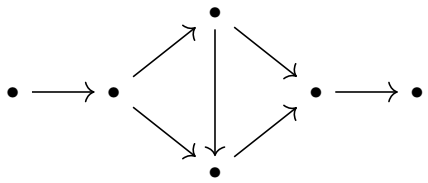
Итак, мы начали с левой коммутирующей диаграммы (= оба треугольника коммутируют = отображения соответственно равны = "≅"сохраняет структуру) и получили правую. Отметим, что правая диаграмма более точно отражает действительную невидимую структуру (одно имя для одной сущности).

2. Второй подход — в обратную сторону. Начав с правой диаграммы, мы добавляем новые обозначения, пока она не станет как слева, т.е. как в начале предыдущего рассуждения.

Точно так же можно анализировать и сокращать любую диаграмму, например, коммутирующий квадрат



можно переписать как $A \to B$ (или как $A \to D, C \to D, C \to B$); таким образом, 5 коммутирующих квадратов из условия 5-леммы[10] превращаются в



что позволяет быстрее осуществлять diagram chasing, без лишних ходов по изоморфизмам. Может быть и обратный случай, когда с целью сохранения квадратности диаграммы один и тот же объект пишут в разных местах и соединяют длинным "= которое с тем же успехом можно воспринимать как стрелку вида ≅.

Далее мы обсудим, есть ли разница между ≅ и =. Очевидно, что нет. Кто-то может сказать "очевидно, да"— и оба будут правы, так как всё зависит от контекста. Например, $\mathbb{Z} = \mathbb{Z}$; что если слева — группа, а справа — кольцо? Или, допустим, мы имеем некоторое A (группа, кольцо, что угодно) и проводим раздельно три цепочки действий (3 эксперимента):

[9] x не переобозначен во что-то вида "$f(x)$"намеренно, чтобы подчеркнуть игру контекстов.

[10] вариант, где 4 вертикальных стрелки — изоморфизмы, см. [Wei94, с. 13]

1. Добавим некоторую структуру к A, затем введём B и скажем, что $B = A$. Обычно в таком случае мы понимаем, что B копирует свойства A: как внутреннюю, так и внешнюю структуру, т.е. взаимодействие с другими объектами. В этом случае $=$ и $\cong$ *могут быть* взаимозаменяемы.

2. Введём знак B, скажем, что $B = A$ и затем добавим структуру к A. В этом случае $B = A$ всё ещё имеет смысл, но использование $\cong$ *может* быть некорректным, т.к. подразумевает равенство и внутреннее, и внешнее, в то время как $=$ относится больше к внутренней структуре или даже её части, например, речь может идти лишь о равенстве множеств. *Может* быть некорректным потому, что мы можем сказать (или это ясно из контекста), что структура, относящаяся к A, индуцируется на B; проблема в том, что это не всегда так. Поэтому, когда мы работаем с двумя обозначениями одного и того же, необходимо следить за согласованностью структур, так как может так оказаться, что введя некоторую структуру на A, мы не индуцируем её на B; может быть и такое, что введение новой структуры ломает уже существующее соответствие, и мы получаем в итоге два разных объекта.

3. Предположим, есть один объект, и мы имеем два его обозначения: A и B, но мы не знаем, что они значат одно и то же. Такой случай возникает, например, в задачах классификации математических объектов. Не зная об этом соответствии, мы можем добавлять структуры к A и B, тем самым нарушая их соответствие.

Смысл в том, чтобы показать, что соответствие между двумя объектами это не априорное и нерушимое или недостижимое свойство, так как некие метаморфозы могут видоизменить изначально разные объекты и они станут одним, так и наоборот, один и тот же объект может преобразоваться в разные сущности. Вспомним, например, разнообразие изоморфизмов (и гомоморфизмов вообще): изоморфизм групп, колец, полей, модулей и т.д. Каждый из них может описывать либо полное соответствие, либо частичное, например, когда мы имеем два кольца, которые изоморфны как группы, но не как кольца; этот пример отражает смысл 3-го сценария. Очевидно, возникает вопрос, насколько устойчива (или, обратно, достижима) идентификация двух объектов в том или ином случае. Универсальное свойство даёт ответ, в частности, в тех случаях, когда мы строим новый универсальный объект, зависящий от A, зная, что $A \cong B$; тогда если для B он уже построен, то он автоматически построен и для A, так как другого быть не может.

Вспомним, что функтор, в частности, сопоставляет объекту некоторой категории объект, возможно, другой категории; так как в математике зачастую конструкции определяются с помощью "уже имеющихся" понятий/-конструкций, единственность определяемого объекта является подозрением на функтор в том смысле, что определение может оказаться случаем "объекту сопоставляется объект"; примером является тензорное произведение.

Литература

Универсальное свойство встречается в теории категорий и гомологической алгебре, поэтому литература та же, что и выше.

Глава 3

Центральные простые алгебры

3.1 Базовые сведения о центральных простых алгебрах

Определение 3.1.1. *R — коммутативное кольцо с 1.* ***R-алгеброй*** *(или* ***алгеброй над*** *R) называется, эквивалентно:*

- *Унитальный правый R-модуль A с заданным на нём R-билинейным отображением $A \times A \to A$, $(x, y) \mapsto xy$, являющимся ассоциативным: $(x(yz) = (xy)z$ для всех $x, y, z \in A$; и для которого есть единица: $1x = x1 = x$.*
- *Кольцо A с единицей и гомоморфизмом из R в центр A.*

Как и в случае с R-модулями, для заданных R и A получаемая R-алгебра A единственна. Как "абелева группа"и "$\mathbb{Z}$-модуль"означают одно и то же, так и "ассоциативное кольцо с единицей"и "$\mathbb{Z}$-алгебра".

Определение 3.1.2. ***Центром*** *R-алгебры A называется множество*

$$Z(A) := \{x \in A \mid xy = yx \text{ для всех } y \in A\}$$

Ясно, что $R \subseteq Z(A)$. При этом

Определение 3.1.3. *R-алгебра A называется* ***центральной*** $\iff R = Z(A)$.

Определение 3.1.4. *R-алгебра A называется* ***простой*** $\iff A \neq 0$ *и её единственными идеалами являются* 0 *и* A.

Первое приближение к пониманию того, что из себя представляют центральные простые алгебры, даёт следующий результат:

Теорема 3.1.1. *A — простая алгебра* $\implies$ *$Z(A)$ — поле.*

Это означает, что рассмотрение центральных простых алгебр над произвольными коммутативными кольцами и над полями — одно и то же: если есть центральная простая алгебра над коммутативным кольцом с единицей, это кольцо есть не что иное как поле. Данный факт также позволяет нам использовать аппарат линейной алгебры: любая F-алгебра является векторным пространством над F.

Из определений выше ясно, что примерами центральных простых алгебр могут служить матричные алгебры. Второе, весомое приближение к пониманию строения центральных простых алгебр даёт следующее утверждение:

Теорема 3.1.2. *[Jah03, с. 18]*

K — поле. Тогда:

1. *A — центральная простая алгебра над K* $\implies$ *существует алгебра с делением D такая, что*

$$Z(D) = K \text{ и } M_n(D) \cong A,$$

где $M_n(D)$ — полная матричная алгебра матриц $n \times n$ с элементами из D;

2. *L — расширение поля K* $\implies$ *$A \otimes_K L$ — центральная простая алгебра;*

3. *K сепарабельно замкнуто и D — конечномерная алгебра с делением над K* $\implies$ *$D = K$.*

Данное утверждение даёт нам следующую картину. Обозначим совокупность всех конечномерных центральных простых алгебр над F через $\mathfrak{S}(F)$. Данную совокупность можно разделить на 2 класса:

1. полные матричные алгебры размерности n^2, $n > 1$ над некоторой алгеброй с делением;

2. алгебры с делением.

С помощью расширений поля F мы можем расщеплять алгебры с делением над F, тем самым превращая их в полные матричные алгебры; это просто видеть, например, из того соображения, что мы можем смотреть на определитель произвольной ненулевой матрицы некоторой алгебры из $\mathfrak{S}(F)$ как на однородный полином; расширение F может дать его нетривиальное зануление и, значит, нетривиальный необратимый элемент — это значит, что алгебра расщепилась. В частности, понятно, что в случае алгебраической замкнутости F алгебр с делением над F, кроме самого F, нет.

Возникает вопрос: как просто заменить все алгебры над F на алгебры над некоторым расширением E/F? Данная процедура называется *расширением скаляров*, и осуществляется с помощью функтора — $\otimes_F E$. Универсальное свойство этого функтора (или: единственность тензорного произведения двух модулей) позволяет нам рассматривать всё те же объекты, но над более широким полем; иначе говоря, мы ставим в соответствие объекту объект, а не совокупность объектов. Тем не менее, после расширения алгебры могут склеиваться в одну в том смысле, что они могут оказаться эквивалентными представителями класса группы Брауэра объемлющего поля. Иллюстрация происходящего — рисунок 3.1.

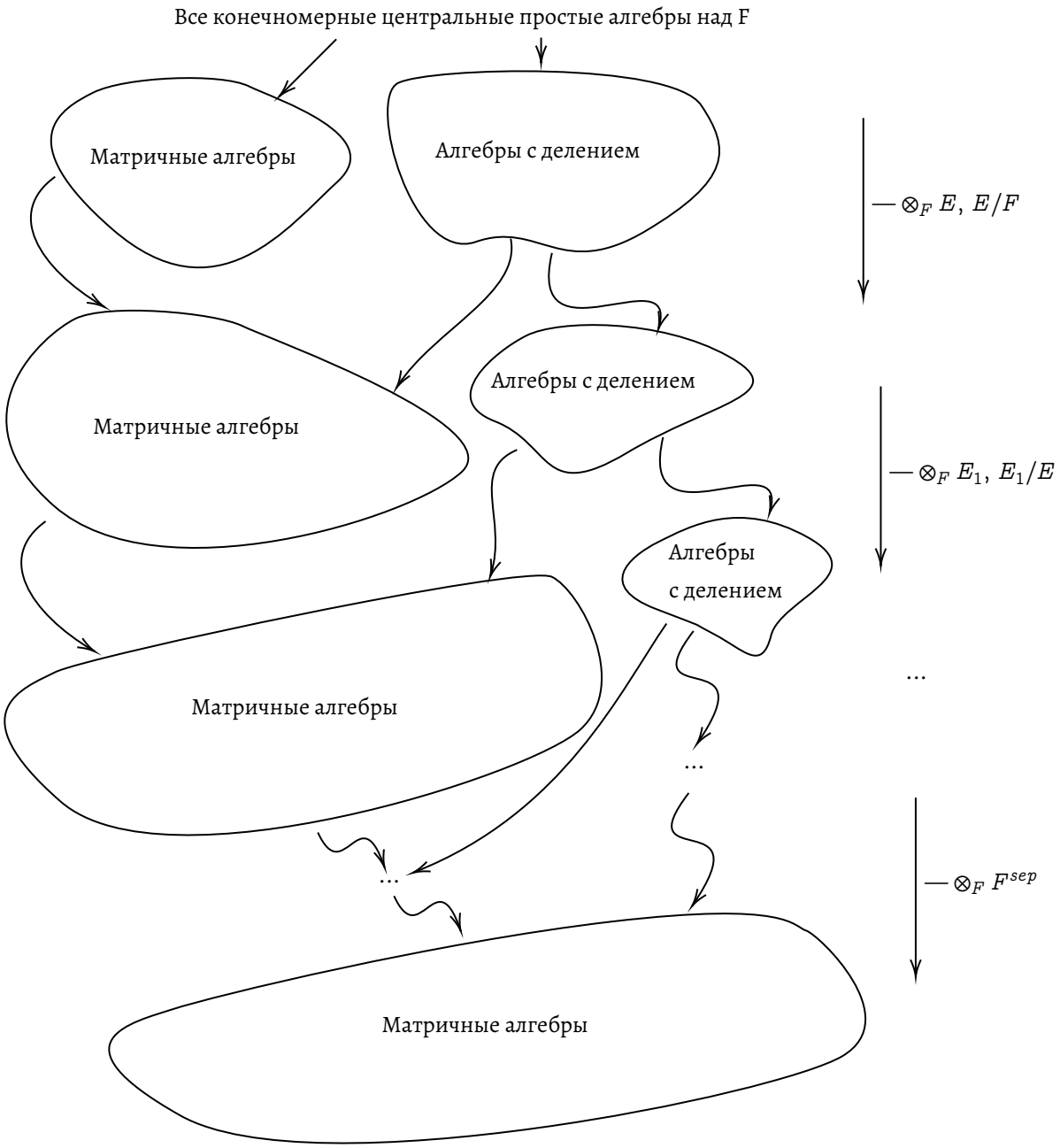


Рис. 3.1: Поведение алгебр при расширении скаляров

3.2 Примеры центральных простых алгебр

1. Любое поле F является центральной простой F-алгеброй. Алгебра с делением, $\dim_F F = 1$.
2. Гамильтоновы кватернионы $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$. Алгебра с делением, $\dim_{\mathbb{R}} \mathbb{H} = 4$: $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$
3. Другая алгебра кватернионов над $\mathbb{R}$: $\left(\frac{1,-1}{\mathbb{R}}\right)$. Полная матричная алгебра размерности 4.
4. Обобщённые кватернионы:

$$\left(\frac{a,b}{F}\right) = F \oplus Fi \oplus Fj \oplus Fk, i^2 = a, j^2 = b, ij = k$$

Гамильтоновы кватернионы являются, таким образом, частным случаем обобщённых кватернионов при $a = b = -1$ и $F = \mathbb{R}$.

Является ли алгебра обобщённых кватернионов матричной алгеброй или алгеброй с делением зависит от a и b. В классификации, а именно, с ответом на вопросы:

1. Изоморфны ли две алгебры с разными a и b?
2. Является алгебра алгеброй с делением или полной матричной алгеброй?

помогают квадратичные формы.

Обозначим через A алгебру обобщённых кватернионов $\left(\frac{a,b}{F}\right)$. Тогда $A = F \oplus A_+$, где $A_+ = Fi \oplus Fj \oplus Fk$ — так называемые *чистые кватерниоы*. Определим норму на A: для элемента $x = c_0 + c_1 i + c_2 j + c_3 k \in A$ сопряжённым к нему будет $x^* = c_0 - c_1 i - c_2 j - c_3 k$, а норма задаётся формулой $v(x) = xx^* = c_0^2 - ac_1^2 - bc_2^2 + abc_3^2$ (как видно, сопряжение и норма задаются по аналогии с $\mathbb{C}$). При $c_0 = 0$, т.е. для $x \in A_+$, $v(x) = -ac_1^2 - bc_2^2 + abc_3^2$. Верно следующее утверждение:

1. A — алгебра с делением $\iff$ формы $c_0^2 - ac_1^2 - bc_2^2 + abc_3^2$ и $-ac_1^2 - bc_2^2 + abc_3^2$ анизотропны, т.е. зануляются только в нуле,
2. A — полная матричная алгебра $\iff$ $c_0^2 - ac_1^2 - bc_2^2 + abc_3^2$ и $-ac_1^2 - bc_2^2 + abc_3^2$ изотропны, т.е. зануляются не только в нуле.

Можно анализировать любую из этих форм и им эквивалентные. Например, для гамильтоновых кватернионов $\mathbb{H}$ ясно, что над $\mathbb{R}$ форма

$$aX^2 + bY^2 - abZ^2 = X^2 + Y^2 + Z^2$$

зануляется только в 0, а потому $\mathbb{H}$ — алгебра с делением. Оказывается, что две алгебры кватернионов над полем характеристики не 2 изоморфны $\iff$ эквивалетны их квадратичные формы (= существует невырожденная линейная замена переменных). Иными словами данный факт также известен как теорема Витта; доказательство можно найти в [SC21, с. 8].

В этом смысле над $\mathbb{R}$ имеется только 2 алгебры кватернионов:

$$\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right) \cong \left(\frac{-2,-1}{\mathbb{R}}\right) \cong \dots \text{ и } M_2(\mathbb{R}) \cong \left(\frac{1,-1}{\mathbb{R}}\right) \cong \left(\frac{1,1}{\mathbb{R}}\right) \cong \dots$$

Это также означает, что $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$.

Менее тривиальным, а потому более интересным примером служат кватернионы над $\mathbb{Q}$. Они полностью классифицированы, и помогают в этом следующие несколько основных результатов и понятий, которые мы дадим и затем обсудим.

Теорема 3.2.1 (**Минковский, Хассе**). *Квадратичная форма изотропна над $\mathbb{Q}$ $\iff$ она изотропна над $\mathbb{R}$ и над $\mathbb{Q}_p$ для всех простых p.*

Доказательство. [Ser96, с. 41] Q. E. D.

Теорема 3.2.2 (**Лемма Гензеля**). *$f \in \mathbb{Z}_p[X]$ — p-адический полином, $\alpha_0 \in \mathbb{Z}_p$ — целое p-адическое число такое, что $f(\alpha_0) \equiv 0 \pmod{p^{2k+1}}$ и $f'(\alpha_0) \not\equiv 0 \pmod{p^{k+1}}$. Тогда существует единственное $\alpha \in \mathbb{Z}_p$ такое, что $f(\alpha) = 0$ и $\alpha \equiv \alpha_0 \pmod{p^{k+1}}$.*

Доказательство. [Q G20, с. 89] Q. E. D.

Данная лемма естественным образом[1] обобщается на случай n переменных:

Теорема 3.2.3. *$F(X_1, \dots, X_n) \in \mathbb{Z}_p[X_1, \dots, X_n]$ — p-адический полином от n переменных, и $\gamma = (\gamma_1, \dots, \gamma_n) \in \mathbb{Z}_p^n$ такое, что $F(\gamma) \equiv 0 \pmod{p^{2k+1}}$ и для некоторого $i = 1, \dots, n$ выполнено $F'_{X_i}(\gamma) \not\equiv 0 \pmod{p^{k+1}}$. Тогда существует $\alpha \in \mathbb{Z}_p^n$ такое, что $\alpha \equiv \gamma \pmod{p^{k+1}}$ и $F(\alpha) = 0$.*

[1] По аналогии с тем, как обобщается основная теорема алгебры на полиномы от n переменных.

Определение 3.2.1. *Для $a, b \in \mathbb{Q}_p^\circ$ определим* ***символ Гильберта:***

$$(a,b)_p = \begin{cases} 1, \ ax^2 + by^2 - z^2 = 0 \text{ имеет нетривиальное решение в } \mathbb{Q}_p, \\ -1, \ \text{иначе.} \end{cases}$$

Теорема 3.2.4. *a, b, c — попарно взаимно простые, свободные от квадратов целые числа. Уравнение*

$$aX^2 + bY^2 + cZ^2 = 0$$

имеет нетривиальное решение в $\mathbb{Q}$ $\iff$ все следующие условия выполнены:

1. *a, b и c не все положительны и не все отрицательны;*
2. *Для каждого простого p, делящего a, существует целое r такое, что $b + r^2 c \equiv 0 \pmod p$; и аналогично для b и c;*
3. *Если a, b и c все нечётны, то сумма некоторых двух из них делится на 4;*
4. *Если a чётно, то $b + c$ или $a + b + c$ делится на 8; и аналогично для b и c.*

Доказательство. [Cas91, с. 20]. Примечательно также, что, как замечено в [QG20, с. 107], условие 1 не используется в доказательстве и следует из 2, 3 и 4. Q. E. D.

Теорема 3.2.5. *p — нечётное простое число, a, b и c — попарно взаимно простые целые числа, не делящиеся на p. Тогда существуют целые x_0, y_0, z_0, не все делящиеся на p, такие, что*

$$ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod p.$$

Доказательство. [QG20, с. 103] Q. E. D.

И также нам понадобится следствие этой теоремы:

Теорема 3.2.6. *p — нечётное простое число, a, b и c — попарно взаимно простые целые числа, не делящиеся на p. Тогда уравнение*

$$aX^2 + bY^2 + cZ^2 = 0$$

имеет нетривиальное решение в $\mathbb{Q}_p$.

Доказательство. Очевидное применение леммы Гензеля, см. [QG20, с. 105] Q. E. D.

Полезный факт 3.2.1. *[Cas91, с. 21]*

$$|a|x^2 + |b|y^2 + |c|z^2 < 4|abc|,$$

где a, b, c — целые числа, свободные от квадратов, а x, y, z — произвольные целые числа.

Обсуждение.

На основе изложенных результатов выделим 3 подхода к классификации кватернионов над рациональными числами:

1. Непосредственное использование теоремы 3.2.4;
2. Использование символа Гильберта и теоремы 3.2.6 (смысл данной теоремы в том, что она позволяет нам сделать классификацию на основе конечного числа проверок: надо посчитать символ Гильберта для нечётных простых чисел, делящих a и b. Примечательно, что для двойки не нужно.);
3. Полезный факт 3.2.1 позволяет перебором найти все "базовые" тройки x, y, z, из которых получаются все решения; тем самым, мы не просто отвечаем на вопрос о наличии или отсутствии решений, а находим их.

Отметим, что лемма Гензеля, помимо её применения для доказательств некоторых приведённых результатов, позволяет строить приближённые решения так, как это делает метод Ньютона. Данная техника называется Hensel lifting, и можно найти соответствующие варианты леммы Гензеля в том числе для полиномов и более общих вариантов. Также использование леммы Гензеля при выводе теоремы 3.2.6 из 3.2.5 показывает, как можно теоретически находить целые решения.

Суть метода поиска целых решений заключается в том, что мы решаем уравнение по какому-то модулю p, затем с помощью леммы Гензеля заключаем, что мы нашли хвост решения, и находим его следующую часть, уже по модулю p^2, и так далее. Пользуясь периодичностью представления целого числа в p-адической записи, мы, встретив потенциальный период, проверяем целое число, дающее такое представление, в качестве решения. Тем не менее, мы не будем использовать такой подход, так как перебор проще.

Итак, запрограммировав описанные выше 3 подхода в Wolfram Mathematica, получаем следующую картинку (одна и та же для трёх разных алгоритмов):

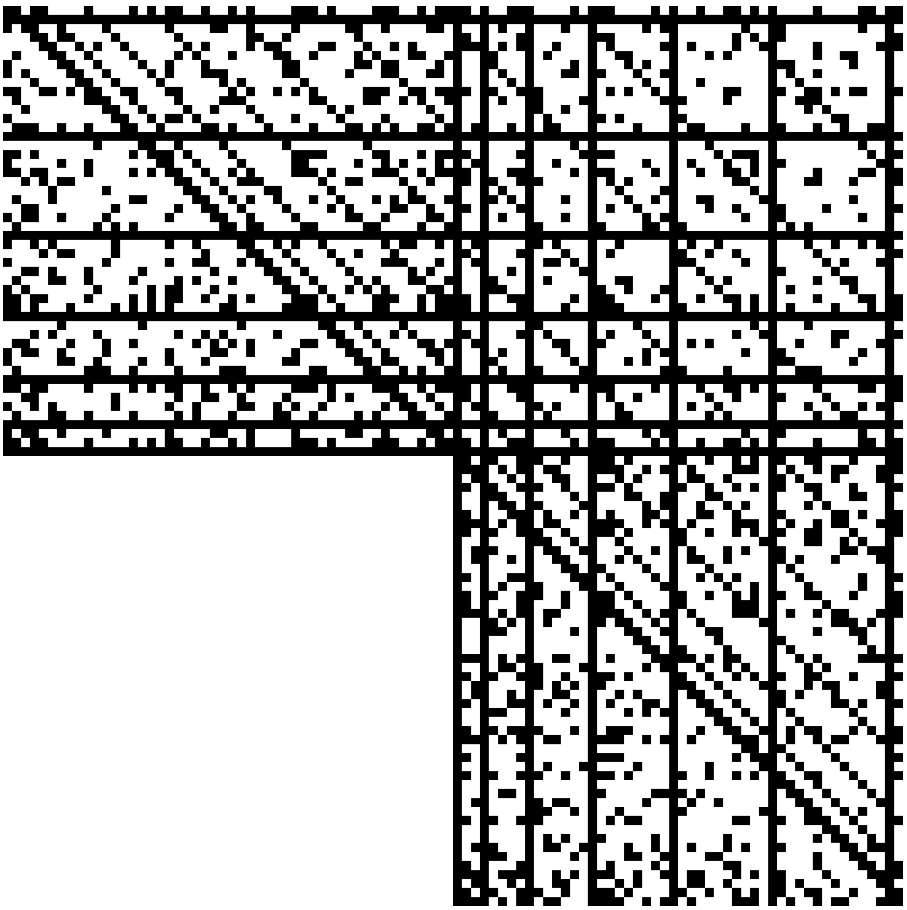


Рис. 3.2: Кватернионы над $\mathbb{Q}$ в диапазоне (-50, -49, …, -1, 1, …, 49, 50) по каждой из осей. Чёрное — одна и та же $M_2(\mathbb{Q})$, белое — возможно, различные алгебры с делением над $\mathbb{Q}$.

Проанализируем, почему картинка именно такая.

1. Белый квадрат в 3 четверти: очевидно, объясняется отрицательностью a и b;
2. Симметричность картинки относительно "оси $y = x$": например, эквивалентность форм $aX^2 + bY^2 - Z^2$ и $bX^2 + aY^2 - Z^2$;
3. Вертикальные и горизонтальные чёрные полосы: свойства кватернионных алгебр $\left(\frac{a,1}{F}\right) \cong M_2(\mathbb{F})$ — чёрные полосы, граничащие с большим белым квадратом, и $\left(\frac{a,bc^2}{F}\right) \cong \left(\frac{a,b}{F}\right)$ — остальные чёрные полосы, появляющиеся при a или b равных 4, 9, 16, …;

4. Первая диагональная чёрная полоса — $a+b=0$ —$\ldots,(-2,2),(-1,1),(1,-1),(2,-2),\ldots$: свойство кватернионов $\left(\frac{a,-a}{F}\right)\cong M_2(F)$

5. Вторая диагональная чёрная полоса — $a+b=1$ — $\ldots,(-1,2),(2,-1),\ldots$: свойство символа Гильберта $(a,1-a)=1$. Обратим внимание также на то, что часть каждой диагональной полосы, проходящей через 1 четверть, сдвинута вниз на 1 клетку относительно своих продолжений в 2 и 4 четвертях, т.к. 0 выкинут.

6. Третья диагональная чёрная полоса — $a+b=4$ —$\ldots,(-1,5),(1,3),(2,2),(3,1),\ldots$; четвёртная диагональная чёрная полоса — $a+b=9$, пятая — $a+b=16$ и т.д. все высшие полосы где $a+b$ — квадраты чисел. Объяснить это можно с помощью квадратичных форм:

   $$aX^2+(n^2-a)Y^2-Z^2=aX^2+n^2Y^2-aY^2-Z^2\sim aX^2+Y^2-aY^2-Z^2=aX^2+(1-a)Y^2-Z^2,$$

   откуда объяснение снова проистекает из свойства символа Гильберта: $(a,1-a)=1$.

Из этих объяснений также видно, что в данном случае языки квадратичных форм, символа Гильберта и свойств кватернионных алгебр взаимозаменяемы и использовать можно то, что удобнее.

Взглянем на картинку побольше:

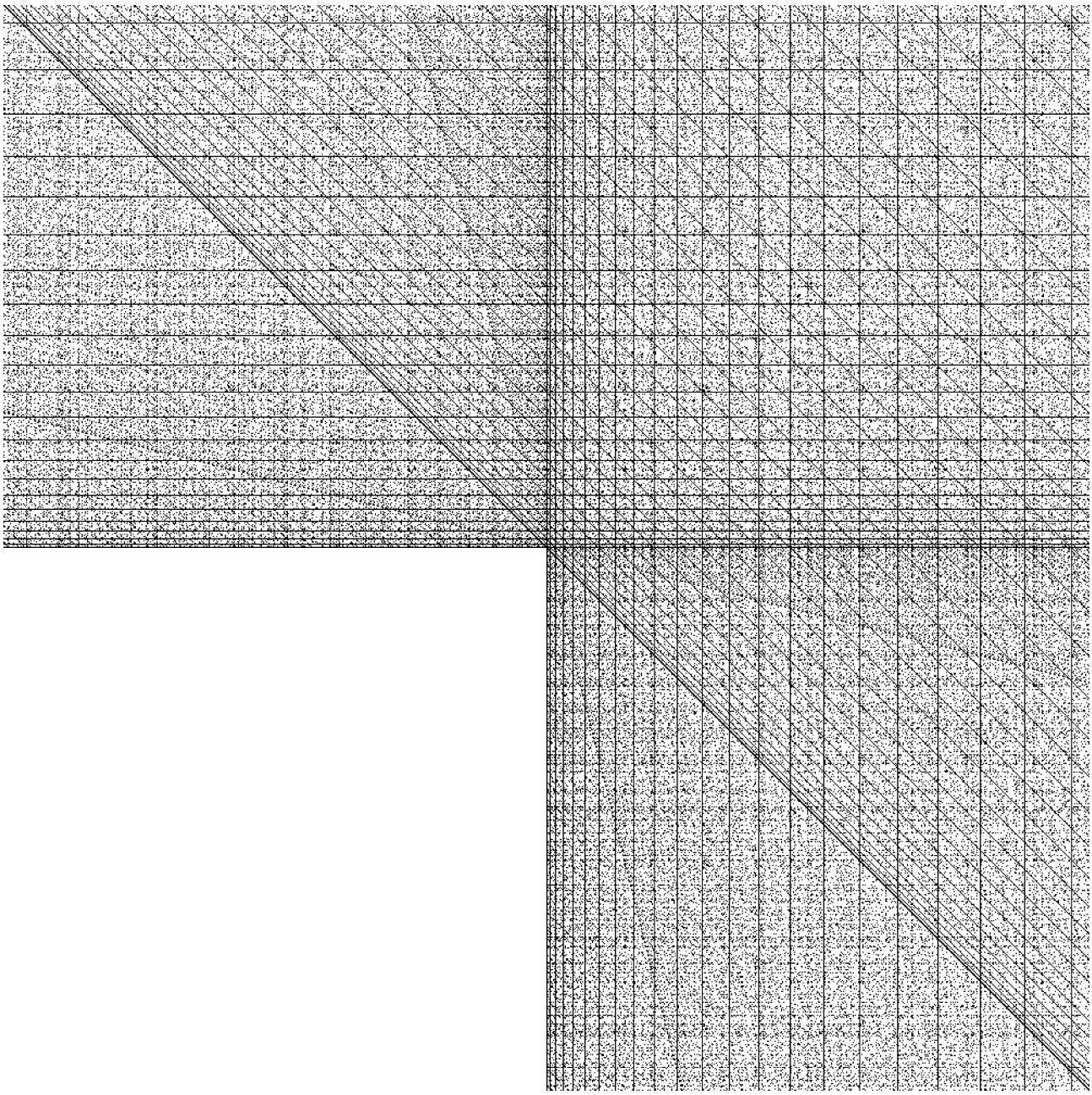


Рис. 3.3: Кватернионы над $\mathbb{Q}$ в диапазоне (-500, -499, …, -1, 1, …, 499, 500) по каждой из осей. Чёрное — одна и та же $M_2(\mathbb{Q})$, белое — возможно, различные алгебры с делением над $\mathbb{Q}$.

Помимо разобранных выше паттернов теперь можно заметить несколько радиальных не сплошных линий. Возникает вопрос: являются ли они явлением некоторого, возможно нетривиального сочетания уже известных свойств или чем-то новым?

Примечательно то, что, скажем, если бы мы не знали некоторых свойств математических объектов, описанных выше, то мы могли бы их найти с помощью гипотез, поставленных исходя из анализа рисунка 3.2, положив, что мы не использовали то, чего "не знаем" , в написании необходимых алгоритмов. Это важный момент, которым мы воспользуемся в обратную сторону: исключим пары (a, b), формирующие уже понятные нам паттерны; тем самым, если радиальные линии исчезнут, мы сможем заключить, что они являются некоторой комбинацией известных формул; в противном случае нам придётся ставить некую гипотезу о существовании формулы, не связанной с чем-то описанным ранее.

Закрасив позиции пар, где a или b не свободно от квадратов, получим

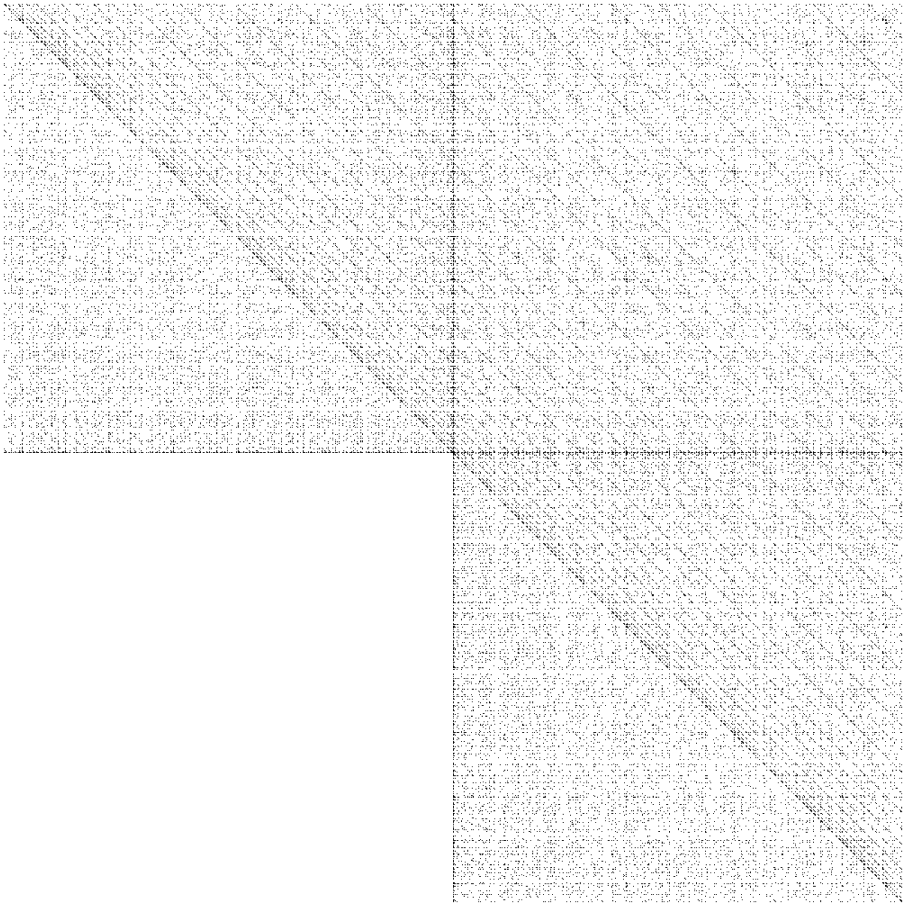


Рис. 3.4: От -500 до 500, пары с квадратами в a или b закрашены белым, как и алгебры с делением.

Видно, что паттерн радиальных линий пропадает, а значит, в этом замешано свойство числа делиться на квадрат. Закрасив белым цветом остальные пары, составляющие знакомые паттерны, получим равномерное полотно:

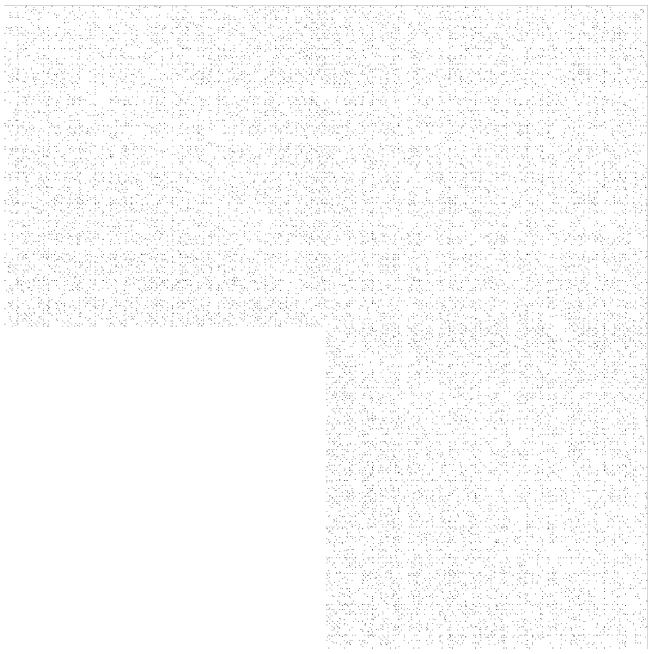


Рис. 3.5: От -500 до 500, белым цветом закрашены пары с всеми понятными свойствами и/или алгебры с делением.

На этом анализ картинок завершён. Отметим, что, возможно, нечто подобное можно применять в случае решения произвольной задачи для постановки гипотез и последующей их проверки: делаем ту или иную визуализацию, изменяем задающий её алгоритм, ставим гипотезу на основании изменения некоторой совокупности паттернов и пытаемся её доказать.

Алгоритмы классификации и генерации картинок вместе с комментариями можно найти в Приложении.

3.3 Группа Брауэра: классический подход

Под группой Брауэра подразумевается один из двух объектов: группа Брауэра поля и группа Брауэра схемы. Мы будем рассматривать только группы Брауэра полей.

Самый простой инвариант объекта, который можно придумать, — это он сам. Однако такие инварианты мало чем полезны для классификации, так как не группируют различные объекты по некоторым общим свойствам.

Группа Брауэра является одним из нетривиальных инвариантов поля, хранящим информацию о расширениях поля и классах центральных простых алгебр. Имеется два подхода к описанию группы Брауэра:

1. Естественный, основанный на рассмотрении совокупности всех центральных простых алгебр и задании необходимых структур; [Pie82, с. 227]
2. С помощью когомологий Галуа, менее естественный подход, но удобный в смысле работы с объектом. [Pie82, с. 253]

Перед тем, как дать теорию, дадим примеры групп Брауэра некоторых полей.

1. $\mathrm{Br}(\mathbb{F}_p) = 0$;
2. Для любого конечного расширения $\mathbb{F}_{p^n}/\mathbb{F}_p$, $\mathrm{Br}(\mathbb{F}_{p^n}) = 0$;
3. $\mathrm{Br}(\mathbb{C}) = 0$; в общем, для любого алгебраически замкнутого поля F, $\mathrm{Br}(F) = 0$;
4. $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$;
5. Для локального поля F имеем $\mathrm{Br}(F) = \mathbb{Q}/\mathbb{Z}$; примерами таких полей могут служить поле p-адических чисел, $\mathbb{Q}_p$, и поле рядов Лорана $\mathbb{F}_{p^n}((t))$;
6. $\mathrm{Br}(\mathbb{Q}) = \left\{(a, x) : a \in \{0, 1/2\}, x \in \bigoplus_p \mathbb{Q}/\mathbb{Z}, a + \sum_p x_p = 0\right\}$;
7. $\mathrm{Br}(k) = 0$, если k — поле типа C_1, см. [SC21, с. 14].

Вспомним наше рассмотрение кватернионов над $\mathbb{R}$: мы неявно полагали, что рассматриваем матричные алгебры размерности ≤ 4; оказывается, других и нет в том смысле, что полные матричные алгебры вне зависимости от их размерности мы будем полагать эквивалентными, а насчёт алгебр с делением имеется следующий любопытный результат:

Теорема 3.3.1 (**Фробениус**). *Каждая конечномерная ассоциативная алгебра с делением над $\mathbb{R}$ изоморфна либо $\mathbb{R}$, либо $\mathbb{C}$, либо $\mathbb{H}$.*

Доказательство. См. [BS19]; в данной статье можно найти как новое элементарное доказательство, так и ссылки на старые. Q. E. D.

Отметим интересную связь: с добавлением структуры банаховой алгебры мы получаем следующий вариант теоремы Гельфанда-Мазура: ненулевая банахова $\mathbb{R}$-алгебра с делением изоморфна либо $\mathbb{R}$, либо $\mathbb{C}$, либо $\mathbb{H}$.

Из теоремы Фробениуса становится понятным описание группы Брауэра для вещественных и комплексных чисел. Тем не менее, для локальных полей и для $\mathbb{Q}$ ситуация менее тривиальна; мы видели описание кватернионных алгебр над $\mathbb{Q}$ и можно ожидать чего-то страшного от группы Брауэра. В самом деле, здесь вовлечена так

называемая теория полей классов, и всюду используются точные последовательности и, соответственно, тут и понадобится описание группы Брауэра через когомологии Галуа.

Итак, изложим необходимую теорию. Начнём с классического подхода.

Обозначим через $\mathfrak{S}(F)$ все конечномерные центральные простые алгебры над F.

Теорема 3.3.2. *Рассмотрим A, B из $\mathfrak{S}(F)$. Следующие условия эквивалентны:*

1. *Существует алгебра с делением $D \in \mathfrak{S}(F)$ и положительные натуральные n и m такие, что*

$$A \cong M_n(D) \text{ и } B \cong M_m(D);$$

2. *Существуют положительные натуральные r и s такие, что $A \otimes M_r(F) \cong B \otimes M_s(F)$.*

Доказательство. [Pie82, с. 227] Q. E. D.

На основе этого имеем

Определение 3.3.1. *Алгебры A и B из $\mathfrak{S}(F)$ называются **эквивалентными**, $\iff$ они удовлетворяют условиям выше. Обозначение: $A \sim B$.*

Полученное фактормножество $\mathfrak{S}(F)/\sim$ и станет нашей группой Брауэра. Для определения нам также потребуется понятие сопряжённой алгебры.

Определение 3.3.2. ***Сопряжённой*** *к R-алгебре A называется R-алгебра A^*, имеющая ту же структуру R-модуля, что и A, но с развёрнутым умножением: $x * y = yx$. Альтернативное обозначение: A^{op}.*

Итак,

Определение 3.3.3. ***Группой Брауэра*** *поля F называется множество $\{[A] : A \in \mathfrak{S}(F)\}$, на котором структура группы задаётся следующим образом:*

1. $[A][B] = [A \otimes B]$ *— операция;*
2. $[F]$ *— нейтральный элемент;*
3. $[A]^{-1} = [A^*]$ *— обратный элемент.*

Доказательство. Нам надо доказать, что определённый нами объект действительно является группой. См. [Pie82, с. 228]. Также из очевидных соображений (свойства $\otimes$) эта группа является абелевой. Q. E. D.

Возникает вопрос: хоть эта группа и абелева, пока неясно, как её считать; сразу неясно даже, какие абелевы группы однозначно не являются группами Брауэра каких-нибудь полей. Например, открытой проблемой является вопрос: для каких натуральных n существует поле F такое, что $|\mathrm{Br}(F)| = n$? [Aue+11, с. 31].

Мы неспроста привели некоторые сведения из классификации абелевых групп: оказывается, группа Брауэра является группой кручения, т.е. является конечно порождённой группой вида $\mathbb{Z}/p_1^{k_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{k_n}\mathbb{Z}$. Этот факт может быть доказан без использования когомологий Галуа, см. [SC21, с. 11—12]. С использованием — [SC21, с. 22].

3.4 Группа Брауэра: подход через когомологии Галуа

Определение 3.4.1. ***Группой Брауэра*** *поля F называется*

$$\mathrm{H}^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\circ),$$

где K^{sep} — сепарабельное замыкание поля K, $(K^{sep})^\circ$ — мультипликативная группа поля K^{sep}.

Имеется также альтернативное описание через относительные группы Брауэра.

Определение 3.4.2. ***Относительной группой Брауэра*** *расширения Галуа L/K называется*

$$\mathrm{Br}(L/K) = \mathrm{H}^2(\mathrm{Gal}(L/K), L^\circ).$$

Определение 3.4.3. ***Группой Брауэра*** *поля K называется*

$$\mathrm{Br}(K) = \operatorname{colim} \mathrm{H}^2(\mathrm{Gal}(L/K), L^\circ).$$

Описание данного копредела именно такое, которое первым приходит на ум; подробное описание можно найти в [Pie82, с. 264—268].

Глава 4

Неабелевы когомологии и соответствие между центральными простыми алгебрами и многобразиями Севери-Брауэра

4.1 Неабелевы когомологии

Обсудим нулевые, первые и вторые когомологии.

Высшие когомологии *G-модулей* (H^i, $i \geq 3$) нам не понядобятся; тем не менее, для $i = 3$ см. [Bro82, с. 102], там же даны ссылки для $i > 3$; отметим, что они получаются простым обобщением: рассматриваются точные последовательности большей длины. Группа Брауэра — главный пример когомологий *G-модулей*, т.е. это когомологии с абелевыми коэффициентами.

Когомологии *G-групп*, т.е. неабелевы когомологии, мы рассмотрим для размерности 0 и 1. Как упоминалось ранее, задание когомологий *G-групп* для $i \geq 2$ представляется проблематичным, см. [Gir71] для соответствующей теории. Основной пример когомологий *G-групп* в нашей теории — множество с отмеченной точкой $H^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathrm{PGL}_n(K^{\mathrm{sep}}))$.

Определение 4.1.1. *A — Γ-множество. Тогда*

$$H^0(\Gamma, A) = A^\Gamma = \{a \in A \mid \sigma a = a \text{ для всех } \sigma \in \Gamma\}$$

Иными словами, нулевые когомологии — Γ-инварианты. Отметим формальное отличие от когомологий в R-mod: в длинной точной последовательности для R-mod в цепочке вместо $H^0(\ldots)$ пишется $\mathrm{Hom}(\ldots)$, тут же будет писаться A^Γ. Это наводит на вопрос: по аналогии с категорией R-mod, будет ли H^1 правым производным функтором от функтора взятия инвариантов? Ответ положителен, согласно [Mil22, с. 94]. Ещё более интересным представляется вопрос: возможно ли построение высших когомологий G-групп с помощью производных функторов?

Дальнейшее определение первых неабелевых когомологий производится с помощью определения 1-коциклов, отфакторизованных по эквивалентности, также определяемой.

Определение 4.1.2. *A — Γ-группа. Тогда* ***1-коциклом в*** *Γ со значением в A называется непрерывное отображение $\alpha\colon \Gamma \to A$ такое, что*

$$\alpha(\sigma\tau) = \alpha(\sigma) \cdot \sigma\alpha(\tau).$$[1]

[1] Скрещенный гомоморфизм в мультипликативной записи, т.к. A — Γ-группа, а не Γ-модуль, т.е. коммутативности не подразумевается.

Множество всех таких 1-коциклов обозначается через $Z^1(\Gamma, A)$. *Отмеченной точкой в данном множестве является отображение, переводящее всё в единицу:* $\alpha(\sigma) = 1$ *для всех* $\sigma \in \Gamma$.

Два 1-коцикла $\alpha, \beta \in Z^1(\Gamma, A)$ *называются эквивалентными (или* ***когомологичными****)* $\iff$ *существует такое* $a \in A$, *что*

$$\beta(\sigma) = a \cdot \alpha(\sigma) \cdot \sigma a^{-1} \text{ для всех } \sigma \in \Gamma.$$

Обозначив через $\sim$ *данную эквивалентность, определим*

$$\mathrm{H}^1(\Gamma, A) = Z^1(\Gamma, A)/\sim.$$

Отметим, что *если* A — Γ-модуль, то $Z^1(\Gamma, A)$ — абелева группа с индуцированной операцией $(\alpha\beta)(\sigma) = \alpha(\sigma)\beta(\sigma)$, и, следовательно, $\mathrm{H}^1(\Gamma, A)$ также является абелевой группой; т.к. сумма/разность скрещенных гомоморфизмов — скрещенный гомоморфизм, а сумма/разность главных скрещенных гомоморфизмов — главный скрещенный гомоморфизм, то $\mathrm{H}^1(\Gamma, A)$ можно альтернативно задать следующим образом.

Определение 4.1.3. A — Γ*-модуль. Тогда*

$$\mathrm{H}^1(\Gamma, A) = \frac{\text{скрещенные гомоморфизмы из } \Gamma \text{ в } A}{\text{главные скрещенные гомоморфизмы из } \Gamma \text{ в } A}$$

Отметим, что в случае Γ-модуля разность скрещенных гомоморфизмов, являющаяся главным скрещенным гомоморфизмом, совместима с эквивалентностью, введённой выше для случая Γ-группы. Действительно, в мультипликативной записи имеем

$$(\beta\alpha^{-1})(\sigma) = a \cdot \sigma a^{-1}$$

для некоторого $a \in A$. Тогда

$$\beta(\sigma)\alpha^{-1}(\sigma) = a \cdot \sigma a^{-1},$$

$$\beta(\sigma) = \underbrace{a \cdot \sigma a^{-1} \cdot \alpha(\sigma)}_{\bullet} = \underbrace{a \cdot \alpha(\sigma) \cdot \sigma a^{-1}}_{\bullet\bullet}.$$

Отметим, что хоть в определении когомологичности 1-коциклов фигурирует $\bullet\bullet$[2], вариант $\bullet$ выглядит более естественным в силу согласованности с гипотетической структурой группы на $\mathrm{H}^1(\Gamma, A)$. Этот нюанс всплывёт далее, т.к. возникает вопрос: что является препятствием для задания групповой структуры на $\mathrm{H}^1(\Gamma, A)$ в случае, когда A — Γ-группа? Дело в том, что в абелевом случае мы беспрепятственно индуцировали операцию на $Z^1(\Gamma, A)$, положив $(\alpha\beta)(\sigma) = \alpha(\sigma)\beta(\sigma)$, потому, что, рассмотрев два раскрытия скобок

$$(\alpha\beta)(\sigma\tau) = (\alpha\beta)(\sigma) \cdot \sigma(\alpha\beta)(\tau) = \alpha\sigma \cdot \beta\sigma \cdot \sigma(\alpha\tau \cdot \beta\tau) = \underbrace{\alpha\sigma \cdot \beta\sigma \cdot \sigma\alpha(\tau) \cdot \sigma\beta(\tau)}_{*},$$

$$(\alpha\beta)(\sigma\tau) = \alpha(\sigma\tau)\beta(\sigma\tau) = \underbrace{\alpha\sigma \cdot \sigma\alpha(\tau) \cdot \beta\sigma \cdot \sigma\beta(\tau)}_{**},$$

в силу коммутативности A не получили дополнительного ограничения из равенства $*=**$. Поэтому лишь подмножество 1-коциклов $\alpha \in Z^1(\Gamma, A)$, где A — Γ-группа, таких, что

$$\beta\sigma \cdot \sigma\alpha(\tau) = \sigma\alpha(\tau) \cdot \beta\sigma,$$

$$\text{для всех } \sigma, \tau \in \Gamma, \beta \in Z^1(\Gamma, A),$$

может быть наделено структурой группы, индуцированной из A. Далее возникает естественное желание выделить из этой новой группы нормальную подгруппу главных скрещенных гомоморфизмов. В этом месте нам понадобится, в частности, $\bullet$ для описания получающейся факторгруппы. Мы оставим дальнейшее явное описание на будущие времена.

[2] И в [Jah03, с. 5], и в [Knu+98, с. 384].

Определение 4.1.4. *A — Γ-модуль.* ***2-коцикл*** *из Γ в A — это непрерывное отображение $\alpha\colon \Gamma\times\Gamma\to A$ такое, что*

$$\sigma\alpha(\tau,\rho)\cdot\alpha(\sigma,\tau\rho)=\alpha(\sigma\tau,\rho)\alpha(\sigma,\tau)\text{ для всех }\sigma,\tau,\rho\in\Gamma.$$

Множество всех 2-коциклов из Γ в A обозначается через $Z^2(\Gamma,A)$. Данное множество является абелевой группой:

$$(\alpha\beta)(\sigma,\tau)=\alpha(\sigma,\tau)\beta(\sigma,\tau).$$

Два 2-коцикла α и β называются эквивалентными (или ***когомологичными****)* $\iff$ *существует непрерывное $\varphi\colon\Gamma\to A$ такое, что*

$$\beta(\sigma,\tau)=\sigma\varphi(\tau)\cdot\varphi^{-1}(\sigma\tau)\cdot\varphi(\sigma)\cdot\alpha(\sigma,\tau)\text{ для всех }\sigma,\tau\in\Gamma.$$

Обозначив через $\sim$ данную эквивалентность, определим

$$\mathrm{H}^2(\Gamma,A)=Z^2(\Gamma,A)/\sim.$$

Примером данного определения является группа Брауэра. Имеется также следующий результат: если A — Γ-модуль, то $\mathrm{H}^2(\Gamma,A)$ является множеством классов эквивалентности расширений Γ с помощью A (соответственно действию Γ на A). Групповая операция на данном множестве называется *суммой Баера*, где нулю соответствует расщепляющееся расширение; см., например, [Wei94, с. 78]. В [Wei94, с. 79] описано упоминавшееся выше естественное обобщение когомологий Γ-модулей для $i\geq 3$. См. также [Rot08, с. 428].

Обсудим далее имеющиеся точные последовательности. В случае когомологий для R-mod длинная точная последовательность получается из леммы о змее; в случае G-mod имеется аналогичная точная последовательность со связывающим гомоморфизмом. Начнём построение с рассмотрения $A\to B\to B/A$.

Если B — Γ-группа, A — Γ-подгруппа в B, то $B/A=\{b\cdot A\mid b\in B\}$ — Γ-множество. Отображение $B\to B/A$ индуцирует отображение $B^\Gamma\to(B/A)^\Gamma$. Далее, $b\cdot A\in(B/A)^\Gamma\iff\sigma b\cdot A=b\cdot A$ для всех $\sigma\in\Gamma$. Класс 1-коцикла $\alpha\colon\Gamma\to A$, определённого как $\alpha(\sigma)=b^{-1}\cdot\sigma b\in A$, $[\alpha]\in\mathrm{H}^1(\Gamma,A)$, не зависит от b, поэтому имеется следующее отображение множеств с отмеченной точкой:

$$\delta^0\colon(B/A)^\Gamma\to\mathrm{H}^1(\Gamma,A),$$

$$b\cdot A\mapsto[\alpha],$$

$$\alpha(\sigma)=b^{-1}\cdot\sigma b.$$

Наконец,

Теорема 4.1.1. *Последовательность*

$$1\to A^\Gamma\to B^\Gamma\to(B/A)^\Gamma\xrightarrow{\delta^0}\mathrm{H}^1(\Gamma,A)\to\mathrm{H}^1(\Gamma,B)$$

точна.

Доказательство. Точность в $(B/A)^\Gamma$: предположим, что 1-коцикл $b^{-1}\cdot\sigma b\in A$ тривиален в $\mathrm{H}^1(\Gamma,A)$, т.е. $\alpha(\sigma)=a^{-1}\cdot\sigma a$ для некоторого $a\in A$. Тогда $ba^{-1}\in B^\Gamma$ и $b\cdot A=ba^{-1}\cdot A$ в B/A является образом $ba^{-1}\in B^\Gamma$.

Точность в $\mathrm{H}^1(\Gamma,A)$: если $\alpha\in Z^1(\Gamma,A)$, $\alpha(\sigma)=b^{-1}\cdot\sigma b$ для некоторого $b\in B$, то $b\cdot A\in(B/A)^\Gamma$ и $[\alpha]=\delta^0(b\cdot A)$. Точность в остальных членах очевидна. Q. E. D.

Более длинная последовательность:

Теорема 4.1.2. *B — Γ-группа, A — Γ-подгруппа в B, и $C=A/B$ (также Γ-группа). Тогда последовательность*

$$1\to A^\Gamma\to B^\Gamma\to C^\Gamma\xrightarrow{\delta^0}\mathrm{H}^1(\Gamma,A)\to\mathrm{H}^1(\Gamma,B)\to\mathrm{H}^1(\Gamma,C)$$

точна.

Доказательство. Точность в $\mathrm{H}^1(\Gamma, B)$: возьмём $\beta \in Z^1(\Gamma, B)$ такое, что $[\beta]$ лежит в ядре последнего отображения цепочки. Тогда

$$\beta(\sigma) \cdot A = b^{-1} \cdot \sigma b \cdot A = b^{-1} \cdot A \cdot \sigma b$$

для некоторого $b \in B$. Значит,

$$\beta(\sigma) = b^{-1} \cdot \alpha(\sigma) \cdot \sigma b$$

для $\alpha \in Z^1(\Gamma, A)$, и $[\beta]$ — образ $[\alpha]$ в $\mathrm{H}^1(\Gamma, B)$. Точность остальных членов доказана в предыдущей теореме. Q. E. D.

Наконец, если B — Γ-группа, A — *центральная* Γ-подгруппа в B, то A — абелева группа, и связывающий гомоморфизм

$$\delta^1 \colon \mathrm{H}^1(\Gamma, C) \to \mathrm{H}^2(\Gamma, A)$$

определяется следующим образом. Для $\gamma \in Z^1(\Gamma, C)$ выберем такое $\beta \colon \Gamma \to B$, что $\beta(\sigma)$ отображается в $\gamma(\sigma)$ для всех $\sigma \in \Gamma$. Рассмотрим отображение $\alpha \colon \Gamma \times \Gamma \to A$, заданное как

$$\alpha(\sigma, \tau) = \beta(\sigma) \cdot \sigma\beta(\tau) \cdot \beta(\sigma\tau)^{-1}.$$

$\alpha \in Z^2(\Gamma, A)$ и соответствующий класс эквивалентности не зависит от выбора $\gamma \in [\gamma]$ и β. Поэтому

$$\delta^1([\gamma]) = [\alpha].$$

Итак,

Теорема 4.1.3. *Последовательность*

$$1 \to A^\Gamma \to B^\Gamma \to C^\Gamma \xrightarrow{\delta^0} \mathrm{H}^1(\Gamma, A) \to \mathrm{H}^1(\Gamma, B) \to \mathrm{H}^1(\Gamma, C) \xrightarrow{\delta^1} \mathrm{H}^2(\Gamma, A)$$

точна.

Доказательство. Точность в $\mathrm{H}^1(\Gamma, C)$: рассмотрим $\gamma \in Z^1(\Gamma, C)$ и β, α такие, как описано выше. Тогда

$$\alpha(\sigma, \tau) = \beta(\sigma) \cdot \sigma\beta(\tau) \cdot \beta(\sigma\tau)^{-1} = a(\sigma) \cdot \sigma a(\tau) \cdot a(\sigma\tau)^{-1}$$

для некоторого $a(\sigma) \in A$. Тогда 1-коцикл $\beta(\sigma) \cdot a(\sigma)^{-1} \in Z^1(\Gamma, B)$, образ которого — γ. Точность в остальных членах доказана выше. Q. E. D.

Данные результаты будут использоваться далее.

4.2 Ключевые вспомогательные теоремы

Теорема 4.2.1 (Сколем, Нётер). *R — коммутативное кольцо с единицей. Тогда $\mathrm{GL}_n(R)$ действует на $\mathrm{M}_n(R)$ сопряжением:*

$$(g, m) \mapsto gmg^{-1}.$$

Если R — поле, то имеется изоморфизм

$$\mathrm{PGL}_n(R) = \mathrm{GL}_n(R)/R^* \cong \mathrm{Aut}_L(\mathrm{M}_n(L)).$$

Доказательство. [Jah03, с. 19], [SC21, с. 20—21], [Pie82, с. 230—231]. Q. E. D.

Иными словами, все автоморфизмы центральной простой алгебры над полем являются внутренними. Прямое применение данной теоремы — доказательство следующей.[3]

[3] С другой стороны, в [SC21, с. 20—21] обратная ситуация: теорема Гильберта 90 используется для доказательства теоремы Сколема-Нётер.

Теорема 4.2.2 (Теорема Гильберта 90). *L/K — расширение Галуа с группой Галуа G. Тогда*

$$\mathrm{H}^1(G, K^*) = 0.$$

Доказательство. [Knu+98, с. 393]. См. также [Pie82, с. 312] для оригинальной формулировки теоремы. Q. E. D.

Основное, но далеко не единственное, применение данной теоремы следующее. Из короткой точной последовательности

$$1 \to K^\circ \to \mathrm{GL}_n(K) \to \mathrm{PGL}_n(K) \to 1$$

получается точная последовательность когомологий

$$\mathrm{H}^1(G, \mathrm{GL}_n(K)) \to \mathrm{H}^1(G, \mathrm{PGL}_n(K)) \to \mathrm{H}^2(G, K^\circ),$$

и, т.к. по теореме Гильберта 90 имеем $\mathrm{H}^1(G, \mathrm{GL}_n(K)) = 0$, то последнее отображение между известными нами объектами (для которых G — абсолютная группа Галуа) имеет тривиальное ядро.

4.3 Многообразия Севери-Брауэра

Многообразия Севери-Брауэра можно задавать несколькими способами. Мы уже видели один из них на примере кватернионных алгебр: соответствующая форма задаётся нормой.

Определение 4.3.1. ***Многообразием Севери-Брауэра*** *называется форма проективного пространства. Точнее: n — натуральное число;* ***многообразием Севери-Брауэра*** *размерности $n-1$ над полем K называется скрученная форма проективного пространства P^{n-1}_K.*

Проблема с явным заданием многообразий Севери-Брауэра в том, что для них необходимо большое количество уравнений. Один из способов задания описан в [Jac96, с. 111—113] и представляется малоприятным нагромождением формул с башнями индексов; там же имеется описание построения примера многообразия Севери-Брауэра кватернионной алгебры, задаваемого 31 уравнением. Также есть статья [Gar20], в которой имеются 2 способа задания с примерами.

Первый способ снова продуцирует большое количество уравнений; его вычислительно сложным местом является нахождение матрицы изоморфизма $\varphi \in \mathrm{GL}_{m+1}(\overline{K})$ из леммы 5.1, [Gar20, с. 5]. Факт, что центральные простые алгебры размерности 2 и 3 являются циклическими, не облегчает нахождение такой матрицы в общем виде с помощью теоремы Гильберта 90, т.к. вовлечены вычисления с необходимостью оперирования определителем матрицы 10 на 10, элементы которой — *символьные* линейные комбинации. Примечательно, что в лемме 5.1 приводится подходящая матрица, но детально не указывается, как она получена; также остаётся вопрос, как найти φ такого вида, чтобы получающиеся далее уравнения были наименее громоздкими. Отметим также, что уравнения вложения Веронезе могут быть гораздо проще (в сравнении с предложением 3.4 из той же статьи) получены из 2 на 2 миноров симметрической матрицы из переменных.

Второй способ даёт *одно* уравнение с помощью норм, [Gar20, с. 9]. См. также [Jac96, с. 138].

4.4 Теоремы о соответствии

Теорема 4.4.1. *L/K — конечное расширение Галуа, $G = \mathrm{Gal}(L/K)$ — соответствующая группа Галуа, n — натуральное число. Тогда существует следующая биекция множеств с отмеченной точкой:*

$$a = a_n^{L/K} : \mathrm{Az}_n^{L/K} \cong \mathrm{H}^1(G, \mathrm{PGL}_n(L)),$$

$$A \mapsto a_A.$$

Доказательство. [Jah03, с. 20] Q. E. D.

Теорема 4.4.2. *L/K — конечное расширение Галуа, $G = \mathrm{Gal}(L/K)$ — соответствующая группа Галуа, n — натуральное число. Тогда существует следующая биекция множеств с отмеченной точкой:*

$$\alpha = \alpha_{n-1}^{L/K} \colon \mathrm{BS}_{n-1}^{L/K} \cong \mathrm{H}^1(G, \mathrm{PGL}_n(L)),$$

$$X \mapsto \alpha_X.$$

Доказательство. [Jah03, с. 24] Q. E. D.

Данные теоремы объединяются в одну, описывающую соответствие между многообразиями Севери-Брауэра и центральными простыми алгебрами.

Теорема 4.4.3. *n — натуральное число, K — поле, A — центральная простая алгебра размерности n^2 над K. Тогда:*

1. *Существует многообразие Севери-Брауэра X_A размерности $n-1$ над K, такое, что выполнено: если L/K — конечное расширение Галуа, расщепляющее A, тогда оно расщепляет и X_A, и имеется один и тот же класс*

   $$a_A = \alpha_{X_A} \in \mathrm{H}^1(\mathrm{Gal}(L/K), \mathrm{PGL}_n(L))$$

   соответствующий A и X_A. Данное условие определяет X_A с точностью до изоморфизма K-схем.

2. *Для соответствия $X \colon A \mapsto X_A$ выполнено:*

   (a) *X совместимо с расширениями K'/K базового поля:*

   $$X_{A \otimes_K K'} \cong X_A \times_{\mathrm{Spec}\, K} \mathrm{Spec} K'$$

   (b) *L/K расщепляет $A \iff L/K$ расщепляет X_A.*

Доказательство. [Jah03, с. 29] Q. E. D.

Следующая теорема любопытна тем, что она отражает явление, которое мы видели на примере с кватернионами: наличие нетривиального решения, точки, означает, что мы столкнулись с матричной алгеброй — но с геометричной стороны.

Теорема 4.4.4. *r — натуральное число, X — многообразие Севери-Брауэра размерности r над полем K, $X(K) \neq \emptyset$. Тогда*

$$X \cong P_K^r.$$

Доказательство. [Jah03, с. 26—27]. Отметим, что тут также используется теорема Гильберта 90 для доказательства. Q. E. D.

Кроме того, упомянутый ранее способ задания многообразий Севери-Брауэра также описывает соответствие с центральными простыми алгебрами и позволяет строить уравнения многообразия Севери-Брауэра по центральной простой алгебре, [Jac96, с. 107—114].

Глава 5

Гипотеза Амицура

5.1 Обзор результатов

Амицуром в работе [Ami55] был сформулирован следующий результат:

Теорема 5.1.1. *Два многообразия Севери-Брауэра бирационально изоморфны* $\Longrightarrow$ *соответствующие классы центральных простых алгебр в группе Брауэра порождают одну и ту же циклическую подгруппу.*

Гипотеза: верна обратная импликация. Результаты и окружающую данную гипотезу теорию можно найти в [Ami55], [Tpe91], [Kra02], [Flo10], [Nov16].

5.2 Возможные пути решения

Имеются мнения, почерпнутые автором из личных бесед, что, вообще говоря, данная гипотеза неверна и существует контрпример; отметим также, что автор неоднократно слышал о невозможности решения данной проблемы, но, тем не менее, когда и кого это останавливало?

Автором намечено несколько стратегий, возможно, имеющих смысл.

Построение цепочек инвариантов

Бирациональные многообразия, вообще говоря, неизоморфны. Тем не менее это тоже своего рода эквивалентность. Существует много различных эквивалентностей и любые два объекта уместно сравнивать с точностью до какой-то эквивалентности; на основании этого предлагается следующее. По двум многообразиям Севери-Брауэра, для которых неизвестно, эквивалентны они или нет, строятся соответствующие объекты-инварианты, такие, для которых понятно, что некоторая их эквивалентность влечёт эквивалентность данных многообразий (или в обратную сторону, или равносильна ей), по которым они построены. Далее строятся объекты-инварианты для первых объектов-инвариантов, тоже со своей эквивалентностью (или набором разных эквивалентностей), и $\Longrightarrow$, $\Longleftarrow$ или $\Longleftrightarrow$ по отношению к предыдущим объектам, и так далее. Данная цепочка может быть выстроена в некотором смысле как набор увеличительных стёкол, где если на некотором шаге цепочки заметно различие объектов-инвариантов рассматриваемого уровня, то это влечёт различие изначальных объектов (и других более низкого уровня), т.е. многообразий Севери-Брауэра. Ясно, что эта стратегия применима к любым двум объектам, которые мы хотим сравнить, например, в рамках решения той или иной задачи классификации, коих огромное число в математике, или же, с точностью до некоторой эквивалентности, все математические задачи являются таковыми (например, любое вычисление отображений куда-то можно полагать поточечной классификацией и т.д.; вообще говоря, видится следующая модель математики: ничего кроме задач классификации и задач по созданию инструментов для решения задач классификации нет; они взаимосвязаны как инь и ян).

Вопрос состоит в том, как закодировать всю необходимую информацию, касающуюся эквивалентности стартовых объектов, в новых объектах. Также, возможно, такие построения инвариантов могли бы иметь функториальный смысл.

Конечность группы Брауэра

Можно рассмотреть явные построения многообразий Севери-Брауэра, центральных простых алгебр и соответствующих элементов в группе Брауэра в случаях, когда она конечна, и на основании этого сделать какие-то общие выводы. Однако вопрос, когда группа Брауэра конечна, является открытой проблемой, и связан с другой открытой проблемой, гипотезой Тэйта-Шафаревича о том, что группа Тэйта-Шафаревича конечна. Известно, что конечность группы Брауэра равносильна конечности группы Тэйта-Шафаревича при определённых условиях, см. Предложение 4.5, [Gro68, с. 118]. См. также [SC21, с. 395]. Возможно, рассмотрение гипотезы Амицура в контексте равносильности конечности группы Брауэра и группы Тэйта-Шафаревича что-то даст.

Приложение А

Код для классификации кватернионных алгебр над рациональными числами и для поиска решений

Classification of quaternions over rationals

by Barodka Mikita

Before proceeding, note that:
1. There is no sophisticated optimization since there is no endgoal in getting the highest performance possible, but solution 2 seems to be a bit faster
2. If you are not acquainted with Wolfram Mathematica, you can merely press “Evaluation → Evaluate Notebook” and make use of manipulates (under “Examples:”)
3. Some of the explanation is placed in my Master’s thesis and is not duplicated here

---

Solution 1

In[1]:=
```
ClearAll@unsquare
unsquare[n_] :=
 Block[{fc = FactorInteger[n]}, Times @@ (fc[[All, 1]]^Mod[fc[[All, 2]], 2])]
 (* removes squares from integers *)
```

Examples:

In[3]:=
```
Manipulate[unsquare@n, {n, 0}] (* input your number and press Enter/return *)
```

In[4]:=
```
ClearAll@alpha
alpha[a_, p_] :=
 Block[{factora = FactorInteger[a]}, If[MemberQ[factora[[All, 1]], p],
   FactorInteger[a][[Position[factora[[All, 1]], p][[1, 1]]][[2]], 0]]
  (* for a=±p1^α1...pn^αn, alpha[a,pi]=αi *)
```

Examples:

In[6]:=
```
Manipulate[alpha[a, p], {a, 20}, {p, 2}]
(* input your numbers and press Enter/return *)
```

In[7]:=
```
ClearAll@hilsymb
hilsymb[a_, b_, p_] := 1 /; a == -b
hilsymb[a_, b_, p_] := 1 /; b == 1 - a
hilsymb[a_, b_, 2] :=
 hilsymb[a, b, 2] = Block[{factora = FactorInteger[a][[All, 1]],
    factorb = FactorInteger[b][[All, 1]], α = alpha[a, 2], β = alpha[b, 2], u, v},
   u = a/2^α; v = b/2^β;
   (-1)^(Mod[(u-1)/2, 2] Mod[(v-1)/2, 2] + α Mod[(v^2-1)/8, 8] + β Mod[(u^2-1)/8, 8])]
hilsymb[a_, b_, p_] := hilsymb[a, b, p] = Block[{factora = FactorInteger[a][[All, 1]],
    factorb = FactorInteger[b][[All, 1]], α = alpha[a, p], β = alpha[b, p], u, v},
   u = a/p^α; v = b/p^β;
   (-1)^(α β Mod[(p-1)/2, 2]) JacobiSymbol[u, p]^β JacobiSymbol[v, p]^α]
   (* Hilbert symbol (a,b)_p *)
```

Examples:

In[12]:=
```
Manipulate[hilsymb[a, b, p], {a, 3}, {b, 3}, {p, 2}]
(* input your numbers and press Enter/return *)
```

Main function:

In[13]:=
```
ClearAll@sol
sol[a_?Negative, b_?Negative] := 1
sol[a1_, b1_] :=
 Block[{a = unsquare@a1, b = unsquare@b1, fc, i}, fc = DeleteCases[
    FactorInteger[a][[All, 1]] ⋃ FactorInteger[b][[All, 1]], u_ /; Abs[u] == 1];
  For[i = 1, i ≤ Length@fc, i++, If[hilsymb[a, b, fc[[i]]] == -1, Return@1, 0, 0]];
  0] (* gives 1 for division algebra and 0 for M_2(ℚ) *)
```

In[16]:=
```
rng = Join[Range@50 - 51, Range@50];
(* range -50, -49, ..., -1, 1, ..., 49, 50 *)
```

In[17]:=
```
res = Reverse@ParallelTable[sol[i, j], {i, rng}, {j, rng}];
```

In[18]:=
```
res // Image
 (* white – possibly non-isomorphic division algebras, black – M_2(ℚ)*)
```

Examples:

In[19]:=
```
Manipulate[sol[a, b], {a, -1}, {b, -1}]
(* input your numbers and press Enter/return *)
```

Solution 2

Main function:

In[20]:=
```
ClearAll@sol2
sol2[a_?Negative, b_?Negative] := 1
sol2[a1_, b1_] :=
 Block[{a = unsquare@a1, b = unsquare@b1, c, fca, fcb, fcc, i}, c = -GCD[a, b];
  a = a/-c;
  b = b/-c; fca = DeleteCases[FactorInteger[a][[All, 1]], u_ /; Abs[u] == 1 ∨ u == 2];
  fcb = DeleteCases[FactorInteger[b][[All, 1]], u_ /; Abs[u] == 1 ∨ u == 2];
  fcc = DeleteCases[FactorInteger[c][[All, 1]], u_ /; Abs[u] == 1 ∨ u == 2];
  For[i = 1, i ≤ Length@fca, i++,
   If[JacobiSymbol[-b ModularInverse[c, fca[[i]]], fca[[i]]] == -1, Return@1, 0, 0]];
  For[i = 1, i ≤ Length@fcb, i++,
   If[JacobiSymbol[-a ModularInverse[c, fcb[[i]]], fcb[[i]]] == -1, Return@1, 0, 0]];
  For[i = 1, i ≤ Length@fcc, i++,
   If[JacobiSymbol[-b ModularInverse[a, fcc[[i]]], fcc[[i]]] == -1, Return@1, 0, 0]];
  If[OddQ[a] ∧ OddQ[b] ∧ OddQ[c],
   If[! MemberQ[Mod[{a + b, a + c, b + c}, 4], 0], Return@1]];
  If[EvenQ[a], If[! MemberQ[Mod[{b + c, a + b + c}, 8], 0], Return@1]];
  If[EvenQ[b], If[! MemberQ[Mod[{a + c, a + b + c}, 8], 0], Return@1]];
  If[EvenQ[c], If[! MemberQ[Mod[{a + b, a + b + c}, 8], 0], Return@1]];
  0]
```

In[23]:=
```
res2 = Reverse@ParallelTable[sol2[i, j], {i, rng}, {j, rng}];
```

In[24]:=
```
res2 // Image
```

Examples:

In[25]:=
```
Manipulate[sol2[a, b], {a, -1}, {b, -1}]
(* input your numbers and press Enter/return *)
```

Solution 3

In[26]:=
```
ClearAll@solv
solv[a_, b_, c_] := solv[a, b, c] = Block[
   {xrange = Range[0, 2 Floor[√Abs[b c]]], yrange = Range[0, 2 Floor[√Abs[a c]]],
    zrange = Range[0, 2 Floor[√Abs[a b]]], brut, res = {}},
   brut = Table[If[a x^2 + b y^2 + c z^2 == 0, AppendTo[res, {x, y, z}]],
     {x, xrange}, {y, yrange}, {z, zrange}];
   Rest@res] (* explicitly finds some of nontrivial solutions *)
```

Examples:

In[28]:=
```
Manipulate[solv[a, b, -1], {a, 7}, {b, 2}]
(* input your numbers and press Enter/return *)
```

Ranges for x, y and z are obtained as follows:

$|a|\,x^2 + |b|\,y^2 + |c|\,z^2 \le 4\,|abc|$

We have maximum possible x iff $y = z = 0$, hence

$|a|\,x \le 4\,|abc|$

$x \le 4\,|bc|$

$x \le 2\left\lfloor \sqrt{|bc|} \right\rfloor$

and similarly for y and z.

In[29]:=
```
ClearAll@easyform
easyform[a1_, b1_] :=
 easyform[a1, b1] = Block[{a = unsquare@a1, b = unsquare@b1, c}, c = -GCD[a, b];
   a = a/-c;
   b = b/-c; {a, b, c}](* for form a1X^2+b1Y^2-Z^2 with arbitrary a1 and b1 gives
    an equivalent form aX^2+bY^2-Z^2 with coprime and square-free a and b *)
```

In[31]:=
```
Manipulate[easyform[a, b], {a, 9}, {b, 24}]
(* input your numbers and press Enter/return *)
```

In[32]:=
```
ClearAll@sol3
sol3[a_?Negative, b_?Negative] := 1
sol3[a_, b_] := If[Length[solv[Sequence @@ easyform[a, b]]] == 0, 1, 0]
 (* no non-trivial solutions = 1, otherwise 0 *)
```

In[35]:=
```
res3 = Reverse@ParallelTable[sol3[a, b], {a, rng}, {b, rng}];
```

In[36]:=
```
res3 // Image
```

Computing for (-500, -499, ..., -1, 1, ..., 499, 500)

In[37]:=
```
rng500 = Join[-Reverse@Range@500, Range@500];
```

In[38]:=
```
res500 = Reverse@ParallelTable[sol[i, j], {i, rng500}, {j, rng500}];
```

In[39]:=
```
res500ni = Reverse@ParallelTable[sol2[i, j], {i, rng500}, {j, rng500}];
```

The 3rd method is omitted for a substantial time is required for computation (since it's brute force seeking for solutions).

In[40]:=
```
res500 // Image
```

Comparing results

In[41]:=
```
res == res2 == res3
```

In[42]:=
```
res500 == res500ni
```

Analysis of pictures

In[43]:=
```
ans = ParallelTable[If[! SquareFreeQ[i] ∨ ! SquareFreeQ[j], 1, sol2[i, j]],
    {i, rng500}, {j, rng500}] // Reverse;
```

In[44]:=
```
ans // Image
```

In[45]:=
```
rng2 = Block[
   {a = DeleteDuplicates[unsquare /@ Range[1000]][[2 ;;]]}, Join[-Reverse@a, a]];
```

In[46]:=
```
ans2 = ParallelTable[If[MemberQ[rng2, i] ∧ MemberQ[rng2, j],
     If[! SquareFreeQ[i + j] ∨ i == 1 - j ∨ i == -j, 1, sol2[i, j]], 1],
    {i, rng500}, {j, rng500}] // Reverse;
```

In[47]:=
```
ans2 // Image
```

Книги

[13] *Homotopy Type Theory. Univalent Foundations of Mathematics*. Princeton, 2013.

[Alu09] Paolo Aluffi. *Algebra. Chapter 0. Second printing*. 2009.

[BC68] Benjamin Baumslag и Bruce Chandler. *Theory and problems of group theory*. 1968.

[Bro82] K. S. Brown. *Cohomology of Groups*. 1982.

[Cas91] J. W. S. Cassels. *Lectures on Elliptic Curves*. Cambridge University Press, 1991.

[Fuc70] László Fuchs. *Infinite Abelian Groups Vol 1*. Academic Press, 1970.

[Gir71] Jean Giraud. *Cohomologie non abélienne*. 1971.

[Gri70] Phillip A. Griffith. *Infinite Abelian Group Theory*. The University of Chicago, 1970.

[Jac96] Nathan Jacobson. *Finite-Dimensional Division Algebras over Fields*. Springer, 1996.

[Kap65] Irving Kaplansky. *Infinite Abelian Groups*. The University of Michigan Press, 1965.

[Knu+98] Max-Albert Knus и др. *The Book of Involutions*. AMS, 1998.

[Lam99] Tsit-Yuen Lam. *Lectures on Modules and Rings*. Springer, 1999.

[LR03] F. William Lawvere и Robert Rosebrugh. *Sets for Mathematics*. Cambridge University Press, 2003. DOI: 10.1017/CBO9780511755460.

[LS09] F. William Lawvere и Stephen H. Schanuel. *Conceptual Mathematics: A First Introduction to Categories*. Springer, 2009.

[Mac12] Antonio Machì. *Groups. An Introduction to Ideas and Methods of the Theory of Groups*. Springer-Verlag Italia, 2012.

[McC00] John McCleary. *A User's Guide to Spectral Sequences*. 2-е изд. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2000. DOI: 10.1017/CBO9780511626289.

[Mil22] J. S. Milne. *Fields and Galois Theory*. Ann Arbor, MI: Kea Books, 2022.

[NSW20] Jürgen Neukirch, Alexander Schmidt и Kay Wingberg. *Cohomology of Number Fields*. Springer New York, 2020.

[Pie82] Richard S. Pierce. *Associative Algebras*. Springer, 1982.

[Q G20] Fernando Q. Gouveâ. *p-adic numbers. An introduction*. Springer, 2020.

[Rij22] Egbert Rijke. *Introduction to Homotopy Type Theory*. 2022.

[Rot08] J.J. Rotman. *An Introduction to Homological Algebra*. Springer New York, 2008.

[SC21] A. N. Skorobogatov и J.-L. Colliot-Thélène. *The Brauer-Grothendieck Group*. Springer, 2021.

[Ser96] J.-P. Serre. *Course in Arithmetic*. Springer, 1996.

[Sha72] Stephen Shatz. *Profinite Groups, Arithmetic and Geometry*. Princeton University Press и University of Tokyo Press, 1972.

[Ste03] Ian Stewart. *Galois Theory. Third Edition*. 2003.

[Vak17] Ravi Vakil. *The rising sea. Foundations of algebraic geometry*. 2017.

[Wei94] Charles A. Weibel. *An Introduction to Homological Algebra*. Cambridge University Press, 1994.

[Айз17] Д. Айзенбад. *Коммутативная алгебра с прицелом на алгебраическую геометрию*. МЦНМО, 2017.

[ГШ18] С. О. Горчинский и К. А. Шрамов. *Неразветвлённая группа Брауэра и её приложения*. МЦНМО, 2018.

[МИ21] Атья М. и Макдональд И. *Введение в коммутативную алгебру*. МЦНМО, 2021.

[Шаф07] И. Р. Шафаревич. *Основы алгебраической геометрии*. МЦНМО, 2007.

Статьи, обзоры, заметки и другое

[Ami55] S. A. Amitsur. *Generic Splitting Fields of Central Simple Algebras*. 1955.

[Aue+11] Asher Auel и др. *Open problems on central simple algebras*. 2011. arXiv: 1006.3304v2 [math.RA].

[BS19] Matej Brešar и Victor S. Shulman. *On, Around, and Beyond Frobenius' Theorem on Division Algebras*. 2019. arXiv: 1912.07846 [math.RA].

[Cho06] Timothy Y. Chow. *You Could Have Invented Spectral Sequences*. 2006.

[Flo10] Mathieu Florence. *Géométrie birationnelle équivariante des grassmanniennes*. 2010. arXiv: 1001.4602 [math.AG].

[Gar20] Elisa Lorenzo García. *Construction of Brauer-Severi Varieties*. 2020. arXiv: 1706.10079 [math.NT].

[Gro68] Groethendieck. *Le groupe de Brauer III*. 1968.

[Jah03] Jörg Jahnel. *The Brauer-Severi variety associated with a central simple algebra: A survey*. 2003.

[Kra02] Daniel Krashen. *Severi-Brauer varieties of semidirect product algebras*. 2002. arXiv: math/0206154 [math.RA].

[Nov16] Saša Novaković. *Rational maps between varieties associated to central simple algebras*. 2016. arXiv: 1602.04444 [math.AG].

[Wil22] Chris Williams. *MA4M3 Local Fields, Lecture Notes*. 2022.

[Yur13] Bilu Yuri. *p-adic numbers and Diophantine equations, Lecture Notes*. 2013.

[Тре91] С. Л. Трегуб. *О бирациональной эквивалентности многообразий Брауэра-Севери*. 1991.