Ministry of Education of the Rebublic of Belarus
Belarusian State University
Mechanics and Mathematics Faculty

Department of Higher Algebra

Barodka Mikita

Severi-Brauer varieties and central simple algebras

Master's thesis

Scientific supervisor
Tikhonov S. V.
associate professor, PhD

Admitted to defense

«____»______________2024 г.

Head of Depatment of Higher Algebra

________________________ Tikhonov S. V.

associate professor, PhD

Minsk, 2024

Contents

Реферат

Магистерская работа содержит 54 с., 5 рис., 51 источник.

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 обсуждаются цели исследования и актуальность, 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. Приводится гипотеза Амицура о бирациональной эквивалентности и обсуждаются возможные стратегии её решения.

Рэферат

Магісцерская праца зьмяшчае 54 с., 5 від., 51 крыніца.

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

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

У першай главе абмяркоўваюцца цэлі даследвання і іпрыводзіцца 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. Прыводзіцца гыпотэза Аміцура аб бірацыянальнай эквівалентнасці і абмяркоўваюцца магчымыя стратэгіі яе вырашэння.

Abstract

This Master's thesis contains 54 pages, 5 pictures, 51 sources.

Keywords: Severi-Brauer variety, central simple algebra, nonabelian cohomology, Amitsur's conjecture, 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 lists the goals of the research, describes the topicality and the reasoning on the gist of this work is given.

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. Amitsur's conjecture on birational equivalence and reasoning on possible strategies for solving it are given.

Chapter 1

Introduction

If you are reading the paper version of this work, the pdf can be found here:
`https://github.com/halva-s-pivom/SBVandCSA`;
Dually, if you are reading the electronic version, the paper one can be obtained by printing it.

1.1 The goals of the research and the topicality

The goal of this work is to analyse the properties of Severi-Brauer varieties and central simple algebras.

Amitsur in his article [Ami55] had stated the following conjecture: two Severi-Brauer varieties are birationally isomorphic $\iff$ the corresponding central simple algebras have the same degree and their classes generate the same cyclic subgroup in the Brauer group. Amitsur proved " $\Longrightarrow$ ", yet " $\Longleftarrow$ " is proven only for particular types of algebras. The case when the algebra is cyclic was considered by Amitsur in Theorem 11.1, [Ami55], and by Roquette in [Roq64]. Roquette had also proven the conjecture for algebras which are crossed products of solvable groups. Some results were obtained by Tregub in [Tpe91]. Krashen in [Kra02] proved the conjecture for algebras with almost cyclic subfields. Partial results are also presented in [Kra08] and [Mat20].

Thus, the topicality may be based on the presence of this fascinating not yet solved problem. Besides, there are applications of the theory of central simple algebras, see the entire book on this [BO13]. As the authors note, division algebras play a key role in the multi-antenna communication, and there are space-time codes based on that theory which are standards of IEEE, see [BO13, pp. vii–viii].

1.2 On the philosophy of this work

During the times of writing this thesis I posed myself an essential question: who would read this work? This is the most vital question because the structure of this work directly depends on the answer. From my personal perspective, many books, articles and other works in mathematics are written without such a consideration, and thus most of them are of the most common form of a dictionary/reference book which consists of blocks like definition-lemma-theorem, definition-definition-theorem-lemma-... and so on, in various proportions and in *linear* order. The linear order of the text, however, is dictated by both the linearity of the natural language itself and the fact of its usage on the paper: even pictures being a nonlinear language appear to be watched page-by-page where they are presented on. Obviously, however, that the only linearity within mathematics is the order of arising of notions in the timeline we live in, as these notions are introduced and developed by us, people, and all we live within the time. That kind of natural motivation of mathematical notions vaporises as the compression is being applied when one writes any paper, clearly, because otherwise we would have had to learn a specific thing for the time it has existed and been elaborated on. So, the problem is: from the one hand, there is a motivation of mathematical objects and their interaction based on the order they were introduced in; from the other hand there are many other connections yet to be discovered which may motivate, too, because of their intrinsic or percepted beauty. Clearly, these miriads of unseen connections form an absolutely nonlinear not even a structure but a sort of chaos. And all we do in mathematics is in fact weaving a rug by our discovery which interlaces itself. So, there is the question: how to keep it all preserved in the text?

This question is a central metaproblem of many written texts in mathematics. By means of this work I'd like to give a partial answer to it. Actually, I'd want to paint the structures taking place here in order to get rid of the linearity of natural language and forms' conditionality so that to more precisely depict the unseen ubiquitous structures of the theory the talk of which will be going on. However, it's unlikely to be done because of both the physical nature and the stiffness of design norms. So, let me just list the objects/notions in the theory of central simple algebras and Severi-Brauer varieties which are like centres of cristallization around which the theory is built.

- a central simple algebra,
- a Severi-Brauer variety,
- $\mathrm{H}^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathrm{PGL}_n(K))$,
- $\mathrm{H}^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^{\circ})$.

The first and the second positions are not surprising (recall the title of this work). Central simple algebras are being dealt with within algebra, so, they are algebraic objects; Severi-Brauer varieties are geometric entities. The third and the fourth positions in the list are taken by very peculiar objects which serve as a bridge (or a translation) between algebraic shapes and geometric shapes, and, therefore, it's algebraic geometry being presented here. Namely, they describe the correspondence between central simple algebras and Severi-Brauer varieties as well as much other information of interest.

The fact that each of these objects listed has its enormous context, namely, books of hundreds of pages on the theory around them, had resulted in me providing many references and discussions, questions, instead of making a sort of compilation. So, central simple algebras, I believe, may interest the reader with quaternions over rationals which are presented in detail. Severi-Brauer varieties are presented mainly via references. As for H^1 and H^2, I had tried to discuss the underlying motivation they possess: cohomology in R-mod motivate group cohomology with abelian coefficients which motivate non-abelian group cohomology.

The most fascinating about this theory is not the fact that there is such a peculiar correspondence between algebraic and geometric objects, but the fact that this correspondence is an example of a more general phenomenon about identification of objects up to something, about object's invariance over its even most different writings. A detailed discussion of such matters will follow. As for my model of seeing things, there are 3 correspondences: the inner, the direct and the outer. First, they are separated by their time of consideration. However, one and the same correspondence may be of any type, for we can consider it in different contexts. In this work we encounter a direct correspondence which means that we are provided with no information about the inner correspondence and the outer one; it's like connecting, identifying two objects with each other without bothering how does this affect as the inner structures like subsets, sub-..., and their interaction, so as the outer ones, which are built upon the lower objects and hence the preservation of compatibility and all alike must be checked. By the outer correspondence I mean, for example, functorial maps. Functorial properties of many things related to this work may be found in the references along the text. However, the most interesting correspondence is the inner one, because it's usually not presented anywhere. For example, the maps between objects are inner with respect to functors; the functor $\mathrm{Hom}(—, A)$ does not touch anything within A; a bijection of sets does not say anything about the correspondence between the subsets of two corresponding to each other elements (guess what is outer and inner here). This inner-direct-outer model is of vital importance, because it explains the fact that given a central simple algebra and the corresponding Severi-Brauer variety, we can choose a subalgebra and a subvariety which do not correspond to each other. That is, subalgebras may not correspond to subvarieties. Clearly, having stated all of this via arrows, the inner can become the outer, and vice versa.

To conclude, whom for is this paper? I presumed that there are two types of people who may read it: unfamiliar with the topic and vice versa. For those who are unfamiliar with, this thesis may give a spark of interest and motivate for further research; for those who are familiar with, I believe, this work may serve as a first-to-read paper to give to those who is new to the subject. Also, many questions, discussions and two strategies for solving Amitsur's conjecture are provided.

Chapter 2

Survey on prerequisites

2.1 Abelian groups

Many objects we will face are abelian groups. Their classification will be useful. Abelian groups are divided into 3 types:

1. **divisible**: a group D is divisible $\iff$ for $x \in D$ and $n \in \mathbb{N}$ there exists such $y \in D$ that $ny = x$;
2. **finitely generated**: a group G is finitely generated $\iff$ there exists a finite set of elements
$$g_1, \dots, g_n \in G,$$
such that any x can be represented as $x = k_1 g_1 + \dots + k_n g_n$, where $k_i \in \mathbb{Z}$;
3. all the others.

We point out that the only group which is both divisible and finitely generated is the trivial one.

Useful fact 2.1.1. *Any divisible group is a direct sum of copies of $\mathbb{Q}$ and $\mathbb{Z}(p^\infty)$ for prime (possibly repeating) p . [Fuc70, p. 104]*

A group $\mathbb{Z}(p^\infty)$ can be written in many ways:

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

that is read from the left to the right respectively as: all non-integer fractions with powers of p in a denominator, a colimit over cyclic groups of order p^n for $n = 1, 2, \dots$, a colimit over groups of roots of 1 of power p^n for $n = 1, 2, \dots$, a factor of p-adic numbers by p-adic integers, a group presentation.

Useful fact 2.1.2. *Any finitely generated group is a direct sum of cyclic groups. [Gri70, p. 15]*

In other words, there are no finitely generated groups distinct from groups of the form

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

where $a \in \mathbb{N}_0$, and p_i may repeat (as well as their powers); there are no divisible groups, too, but of the form

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

where $r_0(D)$ — the torsion-free rank of the group, $r_p(D)$ — the p-rank of the group, see [Fuc70, p. 85]. For a finitely generated group G above, for example, a is its torsion-free rank, and its p-rank — the number of summands $\mathbb{Z}/p\mathbb{Z}$.

The elements of finite order in a group G form a torsion subgroup, denoted $\mathrm{Tor}(G)$; in its turn, the factorgroup $G/\mathrm{Tor}(G)$ does not contain elements of finite order, that is, it is a torsion-free group. For example, in the case of a finitely generated group G we have:

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

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

In this case $G = G/\mathrm{Tor}(G) \oplus \mathrm{Tor}(G)$, that is, "subtraction and addition" works. It holds for divisible groups as well:

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

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

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

The full classification of groups, distinct from finitely generated and divisible ones, is not present yet, and for them "subtraction and addition" of the torsion subgroup may give a group which is different from the initial one.

It turns out that if we go further and "subtract and add" some specifically chosen subgroup (not torsion), troubles may emerge even in the case of finite groups, namely, if the order of a group equals $4, 8, 9, 12, 16, 18, \dots$, that is, if it is divisible by a prime powered in degree ≥ 2. For example, if B is such a group and A — some subgroup in B, then one may expect, that $B = B/A \oplus A$. It's not always the case:

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

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

and so on.

This effect comes up because there exists more than one group of each order as above; namely, if $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$, then there are $k_1 \cdot \ldots \cdot k_m$ of distinct groups of order n; see problem 6.49, [BC68, p. 201]. It is directly related to the so-called **group extensions**. This issue takes place for non-abelian groups as well.

We need the classification above for the following observation. It turns out that cohomology groups are torsion groups; so, computing a cohomology in a finitely presented or divisible cases means finding its writing as $\mathbb{Z}/p_1^{k_1}\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_n^{k_n}\mathbb{Z}$ or $\bigoplus_p \left[\bigoplus_{r_p} \mathbb{Z}(p^\infty)\right]$. Let's list some of the examples vital for our account.

Divisible groups:

1. $\mathbb{Q}$, as seen by definition.

2. $\mathbb{Q}/\mathbb{Z}$ — seen by definition as well, but one can use the fact that a factorgroup of divisible group is again divisible. Also,

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

Useful fact 2.1.3. *The following conditions are equivalent:*

1. *D — a divisible group,*

2. *D — an injective group (or: an injective object in the category of abelian groups; or: in the category of $\mathbb{Z}$-modules),*

3. *a contravariant functor $\mathrm{Hom}_{\mathbb{Z}}(—, D)$ is exact. [Lam99, p. 71], [Wei94, pp. 33–40]*

The second condition implies that if a divisible group is embedded into some group (that is, if it is its subroup[1]), then it can be detached as a direct summand. Hence, if A is a divisible group, then in a short exact sequence of abelian groups $0 \to A \to B \to C \to 0$ we understand, that $B = A \oplus C$.

Literature

- [BC68] — a *masterpiece* of mathematical literature, for it consists of problems, each with a solution; the basic group theory is covered from the ground;
- [Fuc70], [Gri70], [Kap65], [Sha72] — theory of infinite abelian groups, as well as its interaction with homological algebra.

2.2 Modules over rings

We will briefly discuss some of the formal presentations of modules and why it's handy to choose one over another. The key distinction from modules over groups, which we treat further, is that R is an R-module, while a group G is a G-module only in the trivial case $G = 0$. So,

Useful fact 2.2.1. *There are the following equivalent presentations of what an R-module is:*

1. *M — an R-module in a sense of classic definition, see [МИ21, p. 29].*
2. *$R \otimes_R M \cong M$; this writing merely depicts the gist of the word "module": if we take some ring A, which is an R-module, then $A \otimes_R M$ is an A-module; from rings $A_1, \ldots, A_n$ one can form a ring $A_1 \otimes_{\mathbb{Z}} \ldots \otimes_{\mathbb{Z}} A_n$, which is a module over any of these rings, or, in other words, is an $A_1 \otimes_{\mathbb{Z}} \ldots \otimes_{\mathbb{Z}} A_n$-module — again, because any ring is a module over itself.*
3. *$\mathrm{Hom}(R, M) \underset{\text{R-mod}}{\cong} M$ is convenient[2] from the point of dualization: simply reverse the arrows and get $\mathrm{Hom}(M, R)$; when R is a field, the latter writing is nothing but covectors (linear functionals).*
4. *A ring homomorphism is given: $\varphi\colon R \to \mathrm{End}(M) = \mathrm{Hom}(M, M)$.*

Note that: the uniqueness of an R-module M for given R and M = the universal property of $\otimes$ (applied to R and M) = the uniqueness of ring homomorphism $\varphi\colon R \to \mathrm{End}(M)$ (for, φ isn't trivial: $\varphi(0) \neq \varphi(1)$)

Literature

- [Pie82] — a detailed handbook which can be seen as the basic one in the theory we treat in this work;
- [Айз17], [Lam99], [МИ21] — here, one can find as some basic material, so as more advanced one.

2.3 Modules over groups

We are interested in modules over groups in the context of group cohomology. Since modules over a group G (G-modules) form a category, the question arises: how does the description of Hom and $\otimes$ is different for it. One approach is obvious for there is an equivalence of categories:

$$\mathbb{Z}[G]\text{-modules} \cong G\text{-modules},$$

which allows us to set the necessary functors on G-modules by merely inducing them from the category of $\mathbb{Z}[G]$-modules. From the other hand, while the ad-hoc definition of Hom for the category of G-modules is well understood, the question of presence of a genuine analogue of $\otimes$ needs some elaboration on it. We'll leave this question as it is; note that in the context of exposed theory the ad-hoc definition of group cohomology takes place, that is, the approach with inducing from $\mathbb{Z}[G]$-modules is not considered, and that poses a question: is the present ad-hoc definiton equivalent to the induced one? We'll omit that question as is as well and proceed to expose the necessary theory.

[1] We assume $=$ and $\cong$ are the same, the discussion of this is presented further in the text.

[2] Coconvenient or nvenient?

Definition 2.3.1. *A **profinite group** is the limit of finite groups.*

To motivate the introduction of this definition, we present the following **examples of profinite groups:**

1. Any finite group;
2. The absolute Galois group of a number field (that is, of a finite extension of $\mathbb{Q}$);
3. The additive group of p-adic integers.

From now on: Γ is a profinite group. We should point out that there is a topology on it: finite groups possess discrete topology (and that's why they are compact and Hausdorff); hence, Γ — since it's the limit of Hausdorff and compact spaces — is Hausdorff and compact, too. The description of this topology can be found in [ГШ18, p. 47]. This admits an alternative definition of profinite group, see [Sha72, p. 7].

Definition 2.3.2. *A discrete topological space X is called a Γ**-set** $\iff$ Γ continiously acts from the left on X. If X is a group, then X is called a Γ**-group**. And if X — an abelian group — a Γ**-module**.*

We have introduced these 3 different notions to say the following: for a Γ-set A it is possible to define $\mathrm{H}^0(\Gamma, A)$; for a Γ-set A — $\mathrm{H}^0(\Gamma, A)$ and $\mathrm{H}^1(\Gamma, A)$; and $\mathrm{H}^i(\Gamma, A)$ for any $i = 0, 1, \dots$, if A — a Γ-module.

Literature

- [ГШ18] — the theory is presented in lines of exercises; one can find as profinite groups and related objects to it, so as even more related theory;
- [Knu+98] — a comprehensive book, such as [Pie82], but with different covering. One can find a detailed account of objects related to profinite groups.

2.4 Exact sequences. Resolutions

The most natural way of arising of exact sequences can be found in [Айз17, pp. 595–597]. We will discuss a complex

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

and will show that this is indeed a projective resolution for G-module $\mathbb{Z}$ as it's recommended in [ГШ18, pp. 16–17]. By definition,

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

and

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

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

where $\widehat{g_j}$ denotes omitting (literally) the element at position j. One can see from the definition that $G^{\times i} = \overbrace{G \times \dots \times G}^{G \text{ repeats } i \text{ times}}$ is a basis of G-module $\mathbb{Z}[G^{\times i}]$[3], thus it is free and, in particular, a projective object in the category of G-modules. Further, ∂ is indeed a morphism in the category of G-modules and $\partial \circ \partial = 0$ holds, as seen by a routine check:

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

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

[3] That's the gist of definition of $\mathbb{Z}[G^{\times i}]$: we index integers by tuples $(g_1, \dots, g_i)$ and consider their linear combinations.

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

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

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

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

where $\varepsilon = -1$, $\chi = 0$ if $i + 1$ is even, and $\varepsilon = 0$, $\chi = 1$, if odd. Then

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

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

What remains to name our initial complex a projective resolution is to prove its exactness. To this end we'll make use of a homotopy chain equivalence, however, let's start with explaining its mechanism. Consider some objects A, B, C and maps $d_1 \colon A \to B$, $d_2 \colon B \to C$ such that $d_2 \circ d_1 = 0$:

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

that is, we consider a piece of a complex, where homology at B is of our interest. A homology is nothing but a cycle with no boundary, so we take $x \in B$ and having denoted $s_1 = d_1^{-1}$ and $s_2 = d_2^{-1}$ (the sense of that inverses shall become clear from what follows), and analyse its image in C (that's why d_2 acts first and s_2 second) and preimage in A (s_1 first, d_1 second). Then the following variants are possible:

1. **Trivial case:**

$$\begin{tikzcd}
0 \arrow[r, bend left, mapsto, "d_1"] & 0 \arrow[l, bend left, mapsto, "s_1"] \arrow[r, bend left, mapsto, "d_2"] & 0 \arrow[l, bend left, mapsto, "s_2"]
\end{tikzcd}$$

Further assume $x \neq 0$.

2. A cycle with a boundary, that is, x goes to 0 in C, yet it has a nonzero preimage in A:

$$\begin{tikzcd}
0 \neq s_1(x) \arrow[r, bend left, mapsto, "d_1"] & x \arrow[l, bend left, mapsto, "s_1"] \arrow[r, mapsto, "d_2"] & 0 \arrow[dl, bend left, mapsto, "s_2"] \\
 & 0 &
\end{tikzcd}$$

3. **A cycle without a boundary, that is, homology**:

$$\begin{tikzcd}
0 \arrow[dr, bend right, mapsto, "d_1"'] & x \arrow[l, mapsto, "s_1"'] \arrow[r, mapsto, "d_2"] & 0 \arrow[dl, bend left, mapsto, "s_2"] \\
 & 0 &
\end{tikzcd}$$

4. Not a cycle; since $d_2 \circ d_1 = 0$, then $s_1(x) = 0$:

$$\begin{tikzcd}
0 \arrow[dr, bend right, mapsto, "d_1"'] & x \arrow[l, mapsto, "s_1"'] \arrow[r, bend left, mapsto, "d_2"] & d_2(x) \neq 0 \arrow[l, bend left, mapsto, "s_2"] \\
 & 0 &
\end{tikzcd}$$

We observe that 1 and 3 are the **only** cases when d_1s_1 and s_2d_2 give 0 simultaneously! From the diagrams we see, too, that this is equivalent to:

$$(d_1s_1 + s_2d_2)(x) = 0 \iff x \text{ — a homology}$$

and, besides, $(d_1s_1 + s_2d_2)(x) = x$, if x — not a homology. We have:

$$d_1s_1 + s_2d_2 = id \iff \text{there are no homologies in } B.$$

For convenience we will write A, B, C and all the arrows we have into two rows and what we'll get is:

$$\begin{tikzcd}
A \arrow[r, "d_1"'] \arrow[d, "id"'] & B \arrow[r, "d_2"'] \arrow[d, "id"'] \arrow[dl, "s_1"'] & C \arrow[d, "id"'] \arrow[dl, "s_2"'] \\
A \arrow[r, "d_1"'] & B \arrow[r, "d_2"'] & C
\end{tikzcd}$$

Recall that we had started with considering a piece of a complex; so, blocks like the latter assemble to

$$\begin{tikzcd}
\ldots \arrow[r] & A_{i+1} \arrow[r, "d_{i-1}"'] \arrow[d, "id"'] \arrow[dl, "s"'] & A_i \arrow[r, "d_i"'] \arrow[d, "id"'] \arrow[dl, "s"'] & A_{i-1} \arrow[r] \arrow[d, "id"'] \arrow[dl, "s"'] & \ldots \arrow[dl, "s"'] \\
\ldots \arrow[r] & A_{i+1} \arrow[r, "d_{i-1}"'] & A_i \arrow[r, "d_i"'] & A_{i-1} \arrow[r] & \ldots
\end{tikzcd}$$

Let us discuss the further generalization. We are interested not so much in the complex itself, but in its homology; thus it is natural to identify two different complexes if they have the same homologies. From that perspective a complex which is exact is the same as zero complex $\ldots \to 0 \to 0 \to 0 \to \ldots$, and the id map of exact complex is said to be homotopy chain equivalent to zero map. In general, maps f and g of chain complexes are said to be homotopy chain equivalent, if $f - g = \partial s + s\partial$ for some s[4]. We'll use this for proving the exactness of our complex:

$$\begin{tikzcd}
\ldots \arrow[r, "\partial"'] & \mathbb{Z}[G^{\times 3}] \arrow[r, "\partial"'] \arrow[d, shift right, "id"'] \arrow[d, shift left, "0"] \arrow[dl, "s"'] & \mathbb{Z}[G^{\times 2}] \arrow[r, "\partial"'] \arrow[d, shift right, "id"'] \arrow[d, shift left, "0"] \arrow[dl, "s"'] & \mathbb{Z}[G] \arrow[r, "\partial"'] \arrow[d, shift right, "id"'] \arrow[d, shift left, "0"] \arrow[dl, "s"'] & 0 \\
\ldots \arrow[r, "\partial"'] & \mathbb{Z}[G^{\times 3}] \arrow[r, "\partial"'] & \mathbb{Z}[G^{\times 2}] \arrow[r, "\partial"'] & \mathbb{Z}[G] \arrow[r, "\partial"'] & 0
\end{tikzcd}$$

where s is defined $s(g_1, \ldots, g_i) = (e, g_1, \ldots, g_i)$. Check, that $\partial s + s\partial = id - 0 = id$:

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

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

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

where from the beginning and the end of chain of equalities we obtain

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

That is,

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

[4] s may be as the same for different members of the complex, so as be a collection of different s_i.

Hence, we have constructed a projective resolution of $\mathbb{Z}$.

Observe that the most basic example of resolutions is a short exact sequence.

Literature

These are the basic objects of homological algebra, hence the corresponding theory can be found in, for example, [Wei94], [Rot08].

A special role in homological algebra is taken by spectral sequences, because this machinery allows one to compute homology and cohomology; in the context of our theory with their help it is possible to prove many facts about the Brauer group, see [NSW20]. Interesting, with their use it is possible to prove some basic facts as well, for example, snake lemma or 5-lemma, see [Vak17, pp. 62–63]. Apart from a good introduction, [Cho06], we point out a peculiar detail which is, for some reason, is not stated anywhere: levels are written diagonally for handy indexing (same applies to total complex; the fact that the idea of total complex emerge from writing complex members in a graded form is not stated, too); indeed, we write complexes (resolutions, exact sequences) horizontally, hence it's natural to expect a vertical writing of filtrated or graded complex.

2.5 Functors: tensor product, functor of points, Tor, Ext

We'll present a brief discussion on functors which are of our interest. A — some R-module. Our goal is to show how homology and cohomology groups are formed in the case of abelian category, namely, R-mod.

Hom и ⊗

Functor	...-variant	... adjoint	Exact from the ...	Exact from the other side if ...
$— \otimes A$	co	left	right	A is flat
$A \otimes —$	co	left	right	A is flat
$\mathrm{Hom}(—, A)$	contra	right	left	A is injective
$\mathrm{Hom}(A, —)$	co	right	left	A is projective

Derived functors

Functor	...-variant	Derivation
$\mathrm{Tor}_i^R(—, A)$	co	left derived
$\mathrm{Tor}_i^R(A, —)$	co	left derived
$\mathrm{Ext}_R^i(—, A)$	contra	right derived
$\mathrm{Ext}_R^i(A, —)$	co	right derived

One of the functors which plays a key role in our work is contravariant — $\mathrm{Hom}(—, A)$. Let us discuss its adjunction and an emerging nuance.

Theorem 2.5.1. *For any R-module N a functor* $\mathrm{Hom}(—, N)$ *is right-adjoint to itself.*

Proof. [Alu09, p. 536]. Remark: $\mathrm{Hom}(—, N)$ **is not** left-adjoint to itself. Q. E. D.

The nuance is that contravariant $\mathrm{Hom}(—, N)$ should be thought of as a covariant functor from the caterogy which is dual to R-mod — R-mod$^{\mathrm{op}}$; since a limit in R-mod$^{\mathrm{op}}$ is a colimit in R-mod, then the theorem on adjoint functors and limits which we'll present down the text says that $\mathrm{Hom}(—, N)$ saves limits in R-mod$^{\mathrm{op}}$, that is, it saves colimits in R-mod. The substantiality of that remark is that *limits* in R-mod, generally speaking, are not preserved by $\mathrm{Hom}(—, N)$.

Since homology and cohomology groups are objects-invariants in the sense that having two given objects-arguments we get one object in result (as usual, up to isomorphism), during its step-by-step construction it's important that the intermediate objects arising would be unique up to some exactness which keeps the resulting object unique (as well as keep the indermediate objects loose/restricted enough for further constructions).

1. Suppose we are given some R-module A; we want to compute its homology with coefficients in an R-module B. Our first action — to write down A as a complex, concentrated in degree zero. That is, we are now working in the category of complexes of objects from R-mod and that all its members except zeroth position are zero:

$$\begin{tikzcd}
\dots \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & A \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & \dots \\
\dots & n=2 & n=1 & n=0 & n=-1 & n=-2 & \dots
\end{tikzcd}$$

2. Construct a projective resolution as a complexes' morphism, which is but an augmentation map ε:

$$\begin{tikzcd}
\dots \arrow[r] & P_2 \arrow[r] \arrow[d] & P_1 \arrow[r] \arrow[d] & P_0 \arrow[r] \arrow[d, "\varepsilon"] & 0 \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & \dots \\
\dots \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & A \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & \dots \\
\dots & n=2 & n=1 & n=0 & n=-1 & n=-2 & \dots
\end{tikzcd}$$

At this point we pose ourself the questions: does the resolution exist? If there are many of them, how does this fact affect the uniqueness of homology group? The answers are the following theorems:

Theorem 2.5.2. *Any R-module has a projective resolution.*

Proof. [Wei94, p. 34] Q. E. D.

Theorem 2.5.3 (About comparison). *$\varepsilon\colon P_\bullet \to M$ — a projective resolution of M, $f'\colon M \to N$ — a morphism in the corresponding category. Then for any resolution $\eta\colon Q_\bullet \to N$ of N there exists a map $f\colon P_\bullet \to Q_\bullet$ such that $\eta \circ f_0 = f' \circ \varepsilon$ and that f is unique up to chain homotopy equivalence.*

$$\begin{tikzcd}
\dots \arrow[r] & P_1 \arrow[r] \arrow[d, "f_1"] & P_0 \arrow[r, "\varepsilon"] \arrow[d, "f_0"] & M \arrow[r] \arrow[d, "f'"] & 0 \\
\dots \arrow[r] & Q_1 \arrow[r] & Q_0 \arrow[r, "\eta"] & N \arrow[r] & 0
\end{tikzcd}$$

Proof. [Wei94, p. 36] Q. E. D.

As we've discussed earlier, homotopic complexes have the same homology; taken $M = N$ in the latter theorem we get an answer for the question of uniqueness of group homology. See also [Wei94, p. 44].

3. Then, apply the functor $— \otimes_R B$ (or $B \otimes_R —$, since covariance preserves the arrows):

$$\begin{tikzcd}
\dots \arrow[r] & P_2 \otimes_R B \arrow[r] \arrow[d] & P_1 \otimes_R B \arrow[r] \arrow[d] & P_0 \otimes_R B \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & \dots \\
\dots \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & A \otimes_R B \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & \dots \\
\dots & n=2 & n=1 & n=0 & n=-1 & n=-2 & \dots
\end{tikzcd}$$

At this point we note the advantage of a "full" writing as a morphism of complexes: one can easier see why $L_0(F(A)) = F(A)$ $\big($and $R^0(F(A)) = F(A)\big)$:

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

what in our context is translated to $\mathrm{H}_0(A,B) = A \otimes_R B$. By the universal property of $\otimes$ the uniqueness in the sense mentioned above is preserved.

4. Compute homology in the upper row merely by definition as cycles factored modulo boundaries. We get:

$$\begin{tikzcd}
\ldots \arrow[r] & H_2(A,B) \arrow[r] & H_1(A,B) \arrow[r] & H_0(A,B) \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & \ldots \\
 & n=2 & n=1 & n=0 & n=-1 & n=-2 &
\end{tikzcd}$$

In analogous way we obtain cohomology $\mathrm{H}^i(A,B)$:

1. Write B as a complex, concentrated in degree zero. The difference in the arrows' direction has been taken by the change of indexes.

$$\begin{tikzcd}
\ldots \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & B \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & \ldots \\
\ldots & n=-2 & n=-1 & n=0 & n=1 & n=2 & \ldots
\end{tikzcd}$$

2. Construct an injective resolution. There are analogous results about the fact of its existence and about comparison, see [Wei94, p. 40].

$$\begin{tikzcd}
\ldots \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & I^0 \arrow[r] & I^1 \arrow[r] & I^2 \arrow[r] & \ldots \\
\ldots \arrow[r] & 0 \arrow[r] \arrow[u] & 0 \arrow[r] \arrow[u] & B \arrow[r] \arrow[u] & 0 \arrow[r] \arrow[u] & 0 \arrow[r] \arrow[u] & \ldots \\
\ldots & n=-2 & n=-1 & n=0 & n=1 & n=2 & \ldots
\end{tikzcd}$$

3. Afterwards we apply a covariant $\mathrm{Hom}(A, —)$ and get

$$\begin{tikzcd}
\ldots \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & \mathrm{Hom}(A,I_0) \arrow[r] & \mathrm{Hom}(A,I_1) \arrow[r] & \mathrm{Hom}(A,I_2) \arrow[r] & \ldots \\
\ldots \arrow[r] & 0 \arrow[r] \arrow[u] & 0 \arrow[r] \arrow[u] & \mathrm{Hom}(A,B) \arrow[r] \arrow[u] & 0 \arrow[r] \arrow[u] & 0 \arrow[r] \arrow[u] & \ldots \\
\ldots & n=-2 & n=-1 & n=0 & n=1 & n=2 & \ldots
\end{tikzcd}$$

4. From the upper row complex we have

$$\begin{tikzcd}
\ldots \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & \mathrm{H}^0(A,B) \arrow[r] & \mathrm{H}^1(A,B) \arrow[r] & \mathrm{H}^2(A,B) \arrow[r] & \ldots \\
\ldots & n=-2 & n=-1 & n=0 & n=1 & n=2 & \ldots
\end{tikzcd}$$

And similarly $\mathrm{H}^0(A,B) = \mathrm{Hom}(A,B)$.

The difference between homology and cohomology when defining via derived functors is that for homology one needs a projective resolution of any argument, for $\otimes$ is covariant in both of them; meanwhile, to compute cohomology "starting with A" one needs a projective resolution because $\mathrm{Hom}(—, B)$ is contravariant.

Formally that can be stated as follows.

Theorem 2.5.4.

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

Proof. [Wei94, p. 58] Q. E. D.

Theorem 2.5.5.

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

Proof. [Wei94, p. 63] Q. E. D.

Now, we are going to discuss the following substantial theorem.

Theorem 2.5.6 (About adjoint functors and limits). *$L\colon A \to B$ is a left-adjoint functor of $R\colon B \to A$. Then:*

1. *L preserves all colimits;*

2. *R preserves all limits.*

Proof. https://ncatlab.org/nlab/show/adjoint+functor+theorem. Note that in the case of contravariant functor limits go to colimits and vice versa. See [Rot08, pp. 239–240] for a formal definition of preservation. Q. E. D.

In other words, left-adjoint functors commute with colimits; dually, right-adjoint functors commute with limits.

The simplest example to illustrate this is a well-known fact that $(A \oplus B) \otimes C \cong (A \otimes C) \oplus (B \otimes C)$ — "commuting of $\oplus$ and $\otimes$" (or distributivity); left-adjoint functor — $\otimes$; $\oplus$ — a coproduct (an example of colimit). We'll list particular examples of this theorem which are more directly related to our context.

Theorem 2.5.7. *In* R-mod *the following holds:*

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. *$\mathrm{Hom}(\mathrm{colim}\, M_i, B) \cong \lim \mathrm{Hom}(M_i, B)$.*

Proof. [Rot08, p. 241], [Rot08, p. 236], [Rot08, p. 240] Q. E. D.

Since many objects which we face when computing homology (cohomology) are some limits or colimits, we can, by means of the latter statement, split computation of something complex into parts (by carrying a limit/colimit out of the parentheses) and then assemble the results (by taking a limit/colimit).

There are also the following useful results.

Theorem 2.5.8.

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

Proof. [Rot08, p. 418] Q. E. D.

and

Theorem 2.5.9.

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

Proof. [Rot08, p. 419] Q. E. D.

Literature
On top of the previously mentioned ones, [Alu09].

2.6 Categories and equivalences

Briefly speaking, the idea of category is that it is a handy collection of objects which share some common properties. Equivalences between categories should be understood the same way as one understands an isomorphism of algebraic objects: identification ”up to” and the absence of information about identification of ”subobjects”: as a group isomorphism has nothing to tell us about the correspondence between subsets of any two corresponding to each other elements of groups, so as functors say nothing about the correspondence of elements of objects. In this sense categories are ”one level higher” than sets. The place of isomorphism of groups (modules, ...) which preserves the structure is taken by a pair of dually inverse to each other functors, both compositions of which are naturally isomorphic to identity functors in the respective categories. That is, it's all about the same idea of structure preserving.

In this work we encounter the question of classification of objects. Hence it is natural to ask **what** are these objects and **how can they look like** — for, perhaps, they may have already been classified yet in some different representation — the idea of equivalence of categories goes here.

- R-mod — the category of R-modules (R — a commutative ring with 1);
- G-mod — the category of G-modules (G — a profinite group);
- $\mathbb{Z}[G]$-mod — the category of $\mathbb{Z}[G]$-modules;
- Set_G — the category of G-sets;
- BS^K_{n-1} — the category of Severi-Brauer varieties of dimension $n-1$ over a field K, morphisms — isomorphisms of schemes over K;
- $\mathrm{BS}^{/K}_{n-1}$ — the category of Severi-Brauer varieties of dimension $n-1$ over any extension of K, morphisms — composition of an isomorphism of schemes over K and $\mathrm{id} \times \mathrm{Spec}\, a \colon X \times_{\mathrm{Spec}\, L} \mathrm{Spec}\, L' \to X$, where $a \colon L \to L'$ — homomorphism of fields, containing K;
- Az^K_n — the category of central simple algebras over K of dimension n^2; morphisms — isomorphisms of K-algebras which preserve the unity (we point out that Az is written because the generalization of central simple algebras are Azumaya algebras);
- $\mathrm{Az}^{/K}_n$ — the category of central simple algebras of dimension n^2 over any extensions of field K; morphisms — homomorphisms of K-algebras preserving the unity;
- $\mathrm{Mat}^{L/K}_n$ — the category of splitting (that's why it's denoted as Mat) central simple algebras of dimension n^2 over L; morphisms — σ-linear isomorphisms preserving the unity, $\sigma \in \mathrm{Gal}(L/K)$;
- $\mathrm{Sch}^{L/K}$ — L-schemes;
- $\mathrm{P}^{L/K}_{n-1}$ — subcategory in $\mathrm{Sch}^{L/K}$, consisting of L-schemes isomorphic to P^{n-1}_L; morphisms — isomorphisms.

Some equivalences:

- G-mod $\cong \mathbb{Z}[G]$-mod;
- $\mathrm{Mat}^{L/K}_n \cong \mathrm{P}^{L/K}_{n-1}$, see [Jah03, p. 37]. They are antiequivalent as well, see [Jah03, p. 38];

- $\mathrm{Az}_n^{/K} \cong (\mathrm{BS}_{n-1}^{/K})^{\mathrm{op}}$. In particular, $\mathrm{Az}_n^L \cong (\mathrm{BS}_{n-1}^L)^{\mathrm{op}}$ for any extension L/K, see [Jah03, p. 39];
- $\mathrm{Az}_n^K \cong \mathrm{BS}_{n-1}^K$,see [Jah03, p. 43].

See also [Jah03, p. 7].

Literature

For grasping the ideas of category theory there is an excellent book [LS09]. We won't need category theory in its pure form in our context, and the necessary part is covered with the literature on homological algebra stated before.

2.7 Algebras over rings

An algebra over ring is obtained from a module over that ring by one of the equivalent ways:

1. By adding a bilinear map $m\colon A \times A \to A$;
2. By adding a linear map $\mu\colon A \otimes A \to A$.

The equivalence of these two approaches is stated as usual via a commutative diagram:

$$\begin{tikzcd}
A \times A \arrow[rr] \arrow[dr, "m"'] & & A \otimes A \arrow[dl, "\mu"] \\
& A &
\end{tikzcd}$$

Let's make things clear here by specifying the order in which all happens. Given m we state that this diagram commutes and thereupon μ is defined by inducing (the upper arrow is defined by theorem on existence of $\otimes$ of any two modules); conversely, given μ and again by stating that the diagram commutes we obtain m by inducing. The point of considering this little construction is to show its implicit presence in manipulations with $\otimes$. See, for example, [Pie82, p. 179].

Literature

[Pie82] and similar stated above for modules over rings.

2.8 Classic Galois theory. Galois cohomology

Definition 2.8.1. *The* ***absolute Galois group*** *of a field K is, equivalently, any of the following objects:*

1. *The Galois group of K^{sep}/K, where K^{sep} — a separable closure of K;*
2. *The limit over all Galois groups of finite extensions of K.*

The existence and uniqueness of the absolute Galois group for the first case is guaranteed by the following result.

Theorem 2.8.1.

1. *Every field has a separable closure;*
2. *Any two separable closures of a field are isomorphic.*

Proof. [Mil22, p. 117] Q. E. D.

From the second definition one readily sees that an absolute Galois group is a profinite group. There is also a peculiar converse, in a sense, result:

Theorem 2.8.2 (Tate). *Every profinite group G is the Galois group of some Galois extension.*

Proof. [Mil22, p. 132]. We point out that in this proof one finds a construction of such an extension which is, besides, non-unique. Q. E. D.

Further we'll give an answer to the following fascinating question: why does a crossed homomorphism looks like how it does: $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$ (or: $f(\sigma\tau) = f(\sigma) \cdot \sigma f(\tau)$). To this end one needs to read [Mil22, p. 91] in reverse order: we start off with considering a cyclic Galois group G of order n, generated by σ, and we want to have a mutual 1-1 correspondence: $\big($a map $f \colon G \to M\big) \leftrightarrow x \in M$, where M — a G-module and x is a solution for $x + \sigma x + \ldots + \sigma^{n-1}x = 0$[5]. Our goal, in other words, is to to-be-named as "crossed homomorphism" map be defined by its value at the generating element, and vice versa; all that with respect to the latter equation. To achieve this we naturally say that $f(\sigma) = x$, so that the equation turns into

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

In particular we observe that the basepoint $0 \in M$ corresponds to f at the basepoint $\sigma^n = 1$, that is, we have $f(1) = 0$, which is quite what one would expect. Further it is natural to anticipate that f at $\sigma^{n-1}, \sigma^{n-2}, \ldots$ looks like this:

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

$$\ldots$$

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

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

and from the latter equation one readily sees that it is natural to consider maps $f \colon G \to M$ such that

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

Finally, the reason of our desire to construct a correspondence $f \leftrightarrow f(\sigma)$ is that we want to make a construction in G-mod which is absolutely analogous to $\mathrm{Hom}(R, M) \cong M$, where M — an R-module.

Next question: how may crossed homomorphisms look like? One variant is

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

or, since this is true for any $x \in M$,

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

In multiplicative notation:

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

Such a crossed homomorphism is named **principal**. In a sense, as a commutator indicates the non-commutativity, so as a principal crossed homomorphism shows how much the action of G on M is not trivial; this motivates, too. Keeping that in mind we also notice that if M is a trivial G-module, that is, if $\sigma m = m$ for all $\sigma \in G$ and $m \in M$, then any crossed product is a mere homomorphism and any principal crossed homomorphism is trivial, i.e., $f(\sigma) = 0$, as one readily sees from the formulae above.

Literature

An exposition of classic Galois theory with a historical note can be found in [Ste03]. See also [Mil22]. Theory of Galois cohomology can be found in [Knu+98], [NSW20], [SC21].

2.9 The universal property and rewrting

The point of this section is to give a reasoning on the idea of the universal property, the dynamics of objects, their metamorphoses and to answer the question: what does it mean to be equal? We'll consider the following statements:

1. The universal property = the uniqueness of the object being defined.

[5] To be precise, x denotes an actual solution in one case and a variable in the other.

2. $=$ and $\cong$ are one and the same[6].

3. The universal property indicates, possibly, the presence of a functor.

Kernel, direct sum, tensor product [7] are examples of objects which have as classic definitions in the language in which these objects are unique (a map has unique kernel; direct sum of two, say, groups is unique; tensor product is unique), so as in the laguage of category theory, where they are defined as *general* consctructions which coincide with classic definitions in ”understandable” categories, for example in R-mod. Thereupon in categorical definitions of such objects one states that they possess the universal property (= uniqueness in the category language). We've mentioned a **generality** since no ”concrete” category may be stated and hence one needs to check the existence of kernels, direct sums etc. for a concrete category which is of interest. This approach allows (and, at the same time, that's why this approach exists) to broaden the area of usage of some ideas.

Aside from those objects which are defined in term of uniqueness, one knows the converse case, when definition is a pattern which comprises more than one object and hence such objects do not have the universal property (recall a group, a ring, a field, etc.).

The key concept here is **rewriting**. Consider natural numbers constructed via Piano axioms:

1. $1 \in \mathbb{N}$

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

3. ...

where S denotes the function which gives the next element. We've deliberately omitted unnecessary details; the point is that we can write natural numbers as:

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

Immediately we see that even for small numbers the place taken by letters ”S” is more than we'd want to. That motivates us to introduce a new sign, namely, ”2” and say: ”from now on 2 will denote $S(1)$”, i.e. $2 = S(1)$. Now, we can say ”natural numbers” like this:

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

or like that:

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

Situation has got better, though we still have $S(2)$, $S(S(2))$, $S(S(S(2)))$ and other numbers which we'd like to write shorter. That's why analogously we introduce "3", "4", ... and since our memory and/or fantasy are/is limited and natural numbers are infinite, we stop making up new signs and come to the well known decimal system. Therefore, from

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

we've obtained

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

and have saved place on the screen/paper/board by removing S. Besides, the introduction of the decimal system has made the work with natural numbers more *convenient*.

This is an example of **rewriting**.

One depicts this process as follows:

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

[6] This reasoning is conceptual and reflects my vision; after having written these ideas I had discovered, as it turned out, that they are related to HoTT (Homotopy Type Theory); namely, the given discourse about identification of $=$ and $\cong$ is known as Voevodsky axiom which is of importance in HoTT. Ideas like rewriting/computation have their names too (λ-abstraction, β-rule, η-rule, ...). See [13] and [Rij22].

[7] In a suitable category.

What if we reverse the situation?

Imagine having $1, 2, 3, \ldots$. Imagine too that for some reason we want to obtain that strange notation with ”S”. One readily sees that the reasoning above is reversible, so, the inverse *rewriting* looks like this:

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

The difference is that we've taken some properties from the silent (unspoken, implicit, etc.) part of the context and actually said them, i.e. converted the implicit into the explicit. It's also clear that we can rewrite with any other notation:

$$1 \rightsquigarrow a$$

$$2 \rightsquigarrow b$$

$$\ldots$$

or, vice versa, we could've started with a meaning ”one” , b, meaning ”two” , and so on. The point is: *an object does not depend on the way we write it.* Here are several equivalent statements:

1. An object is invariant over the signs denoting it, that is, no matter how we write it — it remains the same.
2. We can compute: computation is nothing but rewriting in more *convenient* sings; for example, rewriting $2+2$ to 4, rewriting group as a direct sum of $\mathbb{Z}$ and its factors and so on. In other words the point of any computation (= rewriting) is to obtain a more convenient representation with signs. In particular, $\sqrt{2}$ is already computed (tautologically) for some people, but for others its computation would be its rewriting as $1.4142\ldots$. It depends!

There is more. Denote some rewriting of A into B as $x\colon A \leftrightsquigarrow B$. Yet we know many other letters, signs and symbols and could've written this rewriting as $y : A \leftrightsquigarrow B$. It's absolutely clear that x and y do the same thing: they tell us that A and B can be rewritten to each other; clearly, x and y denote the same object! In the same manner we can rewrite rewritings, say, z — a rewriting of x into y, i.e. $z\colon x \leftrightsquigarrow y$. It's clear that one can continue this process up to infinity: rewrite rewritings of rewritings, etc.

That's **exactly** what does the universal property say.

Consider an example of notion of a product in categorical terms: for objects A and B there exists an object *denoted* $A \times B$ together with maps $A \times B \to A$ and $A \times B \to B$. The following diagram is usually drawn:

$$\begin{tikzcd}
A \times B \arrow[r] \arrow[d] & A \\
B &
\end{tikzcd}$$

Question: have we just said that this construction depends on A, B and $A \times B$, i.e., are these the only signs we can use for denoting the product? or is the product defined solely for A and B? Obviously not. It's always been clear from the context that different definitions involve different notations yet they mean the same thing. What is more interesting is that notations may differ so much that rewriting of one thing to the other becomes a theorem and even more: at times, rewriting can be an unsolved problem of classification.

Our goal is to diminish the silent part of the context, to make the implicit explicit. To this end we'll refine the definition of product we've given above. Consider 2 approaches:

1. We say that if there is some object denoted C which is *the same*, as $A \times B$, along with morphisms $C \to A$ and $C \to B$, which are *the same*, as $A \times B \to A$ and $A \times B \to B$ respectively, then the whole product is the same with

initial one; one draws the following diagram:

$$\begin{tikzcd}
C \arrow[drr, bend left, "pr'_A"] \arrow[dr, dashed, "\exists!", "\cong"'] \arrow[ddr, bend right, "pr'_B"'] & & \\
& A \times B \arrow[r, "pr_A"] \arrow[d, "pr_B"] & A \\
& B &
\end{tikzcd}$$

and says: ”it commutes”. Let’s explain what’s happened.

”$A \times B \to A$ is the same with $C \to A$” means that there is *some* morphism and we know two of its names (two phenomena, two links, two presentations, etc.); denote it by $pr_A : A \times B \to A$ and $pr'_A : C \to A$. Since we are considering one morphism, we conclude than C and $A \times B$ denote the same object. But what if pr_B and pr'_B were different? Then, at least, we would not have an ability to identify two products; it could’ve turned out, too, that C and $A \times B$ would denote different objects; yet this is not our case.

Let’s discuss the diagram.

Dashed arrow $\dashrightarrow$ means that there exists a morphism but it’s not been set (not given). This is another example of rewriting which is denoted as $\cong$ and called an *isomorphism*. The sign ∃! points out that this map fits into our conventions of rewriting, i.e., this is not a *symbol*, but a mere *sign*. As we know, ∃! is usually understood as ”there exists a unique something” which is in its turn means that it’s unique up to isomorphism which is unique up to etc. (rewriting of rewritings of rewritings…).

Then, what does ”the diagram commutes” mean? Usually the arrow → means that we are transforming one object into another one innerly, like the simplest map between sets. From this point of view → may be regarded as a collection of arrows ↦. In its turn ↦ can be viewed as an isomorphism[8] (rewriting), since it connects *points*, that is, some entities, which inner structure at the time of consideration is not of our interest.[9]

Let’s focus on $A \times B, C, A$ and on maps between them. Since $A \times B$ and C are one and the same object, we pick a point in it and give it a name, say, x, and see where it goes by arrows ↦ belonging to pr_A and pr'_A. However, recall that pr_A and pr'_A are one and the same, that is, it’s a single map, and hence we get the following picture:

$$\begin{tikzcd}
C \arrow[dr, "pr'_A"] \arrow[dd, dashed, "\exists!\cong"'] & & & & x \arrow[dr, mapsto] \arrow[dd, mapsto] & \\
& A & {} \arrow[r, "\text{pick a} \mapsto"] & {} & & x \\
A \times B \arrow[ur, "pr_A"'] & & & & x \arrow[ur, mapsto] &
\end{tikzcd}$$

This is a commuting triangle.[10] When all the triangles, squares, etc. commute in a diagram, we say that the whole diagram commutes. Formally, having denoted $C \to A \times B$ as f, the sense of the right one picture can be said as

[8] One can ask: what if there are two points which are mapped into the other one? Which ↦ to choose then for the inverse? There are at least two possible answers: the first is, for example, that if we are in the category of R-modules or alike, then the inverse ↦ arrow is chosen according to a canonical representative of an equivalence class. The second is more interesting: the solution is that each ↦ belongs to its own context which does not interfere with the others; we don’t bother about many other linear maps when considering a sole linear map between linear spaces — why should we then be bothered by some other ↦ arrows?

[9] Indeed, despite the fact of possibility of sets of sets of … ierarchy, we always deal with only 2-leveled ierarchy of the type ”set-points”. Perhaps, one can be more comfortable with regarding ↦ as an isomorphism of trivial groups or some other identification of trivial structures (that is, they are trivial in *this particular* context).

[10] x has not been rewrited into something like ”$f(x)$” deliberately in order to emphasise the context game.

$pr'_A = pr_A \circ f$. Since f is our rewriting, an identification of names, it's clear that we can rewrite it as id, that is, $\dashrightarrow$ dissapears/contracts. The latter composition becomes $pr'_A = pr_A$. The same reasoning applies to B together with its arrows and we get another commuting triangle and $pr_B = pr'_B$. In the end, we get rid of pr'_A and pr'_B, since they have no new information for us (for they are the same as pr_A and pr_B respectively). Depiction of our procedure:

$$\begin{tikzcd}
C \arrow[dr, dashed, "\exists!\cong"] \arrow[drr, bend left, "pr'_A"] \arrow[ddr, bend right, "pr'_B"'] & & \\
& A \times B \arrow[r, "pr_A"] \arrow[d, "pr_B"] & A \\
& B &
\end{tikzcd}
\longrightarrow
\begin{tikzcd}
C \arrow[r, bend left, "pr_A"] \arrow[r, bend right, "pr'_A"'] \arrow[d, bend right, "pr'_B"'] \arrow[d, bend left, "pr_B"] & A \\
B &
\end{tikzcd}
\longrightarrow
\begin{tikzcd}
C \arrow[r, "pr_A"] \arrow[d, "pr_B"'] & A \\
B &
\end{tikzcd}$$

Having started with the left commuting diagram (= both triangles commute = "≅" preserves the structure) we've obtained the right one. Note that this right diagram in a sense is closer to the actual structure (one name for one entity).

2. The second approach is backwards. Having started with the right diagram in the latter picture, we add new signs until it gets as it was at the start of the previous reasoning.

The same way one can analyse and contract any suitable diagram, for example, a commuting square

$$\begin{tikzcd}
A \arrow[r] \arrow[d, "\cong"'] & B \arrow[d, "\cong"] \\
C \arrow[r] & D
\end{tikzcd}$$

can be rewritten to $A \to B$ (or $A \to D, C \to D, C \to B$); hence, 5 commuting squares from the statement of 5-lemma[11] are being transformed into

$$\begin{tikzcd}
& & \bullet \arrow[dd] \arrow[dr] & & \\
\bullet \arrow[r] & \bullet \arrow[ur] \arrow[dr] & & \bullet \arrow[r] & \bullet \\
& & \bullet \arrow[ur] & &
\end{tikzcd}$$

and that allows to make a diagram chasing faster, without unnecessary moves. There is also a reverse situation when one wants to keep the diagram squared and to this end one and the same object is written in different places and a long "=" is written then as an arrow. Equally we could've used "≅".

So, is there any difference between ≅ and =? Obviously, not. One may argue and say "yes" — and both answers will be correct as they depend on the context.

For example: $\mathbb{Z} = \mathbb{Z}$; what if the left one is a group and the right one is a ring? Or, imagine having some A (group, ring, anything; whatever) and conducting three lines of actions: (like 3 experiments):

1. Add some structure to A, then introduce B and say: $B = A$. Usually in this case we implicitly understand that B copies the properties of A: both the inner and outer structures, that is, its behaviour with other objects. Then $=$ and ≅ *may be* mutually replaceable.

[11] A version where 4 vertical arrows are isomorphisms, see [Wei94, p. 13]

2. Introduce the sign B, say that $B = A$, and then add some structure to A. In this case $B = A$ may still remain correct, but $\cong$ *may* be incorrect since it usually refers to identification of both inner and outer structure whereas $=$ is more about the inner one, for example, $=$ may refer to a mere equality of sets. Again, *may* be correct or incorrect because we can say (or it is understood from the context) that the structure related to A is being unduced on B; the problem is that it's not always so. Thus we should keep track of structures and their relation to each other, namely, their mutual compatibility — when working with many signs — as it may turn out that having introduced a new structure to some sign, we may lose (or acquire) some of identities or equivalences.

3. Assume there is a single object two names of which are given: A and B. However we don't know that they denote one and the same thing; this is the case with classification problems. Not knowing about existing equivalence between signs, we can add something to one of them and break the equivalence.

The point is: any sort of equivalence, both given or to be discovered is not an apriori property nor something unachievable, for some metamorphoses can change initially different objects so that they become one, and vice versa, one and the same object can split into many different entities-notations, seen or unseen.

Recall the diversity of isomorphisms: of groups, of rings, of fields, etc. Each of them may refer to either the full identification or a partial one. For example, two rings may be isomorphic as groups yet not as rings themselves; with different formulations, this illustrates the three scenarios which are actually one and the same idea stated in slightly different words.

Clearly, the question follows: how steady an identification (or, dually, how achievable) of two objects is in one or the other case. The universal property provides an answer, in particular, when we build some new object which depends on A which possesses the universal property; then for any B such that $A \cong B$ the object is automatically built (by inducing) as no other such can emerge.

Recall that any functor, in particular, gives a connection between objects from possibly different categories. As many objects in mathematics are built using some already been built ones, the uniqueness of an object makes us inclined to think that the building of this object is a functor in a sense that we get some object from another one; an example of that is tensor product. This justifies the statement that the universal property may tell us that there is some functor around.

Literature

The universal property takes place in category theory and homological algebra, so the literature is the same as above. However, any explanations of my philosophy exposed here and further elaborations on it can be obtained from a personal conversation with me, the author.

Chapter 3

Central simple algebras and the Brauer group

3.1 The basics of central simple algebras

Definition 3.1.1. *R — a commutative ring with 1. An **R-algebra** (or **an algebra over** R) is, equivalently:*

- *A unital right R-module A with a R-bilinear map $A \times A \to A$, $(x, y) \mapsto xy$, which is associative: $x(yz) = (xy)z$ for any $x, y, z \in A$; and for which there is a unity: $1x = x1 = x$.*
- *A ring A with unity and a homomorphism from R to the centre of A.*

Like in the case with R-modules, for given R and A the resulting R-algebra A is unique. As "abelian group" and "$\mathbb{Z}$-module" mean the same thing, so as for "associative ring with unity" and "$\mathbb{Z}$-algebra".

Definition 3.1.2. *The **centre** of an R-algebra A is*

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

Clearly, $R \subseteq Z(A)$. Besides,

Definition 3.1.3. *An R-algebra A is called **central** $\iff$ $R = Z(A)$.*

Definition 3.1.4. *An R-algebra A is **simple** $\iff$ $A \neq 0$ and its only ideals are 0 and A.*

The first approximation to seeing what a central simple algebra is is given by the next result:

Theorem 3.1.1. *A — a simple algebra $\implies$ $Z(A)$ — a field.*

This means that considering of central simple algebras over arbitrary rings or fields is the same thing: if there is any central simple algebra over ring with unity, then that ring is a field. This fact lets us use the machinery of linear algebra, because any F-algebra is a vector space over F.

From the definitions above one readily sees that matrix algebras are examples of central simple algebras. Are there any other? See next.

The second approximation to understanding of central simple algebras is given by:

Theorem 3.1.2. *[Jah03, p. 18]*

K — a field. Then:

1. *A — a central simple algebra over K $\implies$ there exists a division algebra D, such that*

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

where $M_n(D)$ — a full matrix algebra, $n \times n$, with entries in D;

2. *L — an extension of K $\implies$ $A \otimes_K L$ — a central simple algebra;*

3. *K is separably closed and D — a finite-dimensional division algebra over K $\implies$ $D = K$.*

This gives us the following picture. Denote all finite-dimensional central simple algebras over F by $\mathfrak{S}(F)$. This collection can be split into 2 classes:

1. full matrix algebras of dimension n^2, $n > 1$ over some division algebra;

2. division algebras.

There goes the question: how to accurately convert algebras over F into algebras over some extension E/F? Such a procedure is called a *scalar extension*, and is being done by means of a functor — $\otimes_F E$. The universal property of this functor (or: uniqueness of tensor product of two modules) allows us to consider the same objects over a wider field; in other words, an object goes to an object, not a collection of them. Nevertheless, after the extension two algebras may glue together into one in a sense that they can become equivalent representatives of a class in the Brauer group of extension field. We can regard the determinant of an arbitrary non-zero matrix in some algebra in $\mathfrak{S}(F)$ as a homogeneous polynomial; an extension of F may give its non-trivial root and, therefore, a non-trivial non-inversable element. Conversely, a non-trivial root is preserved by extensions. Clearly, when extending up to the algebraic closure, all algebras glue together into one in a sense as above. Basing on that, here is a picture 3.1 of what's going on.

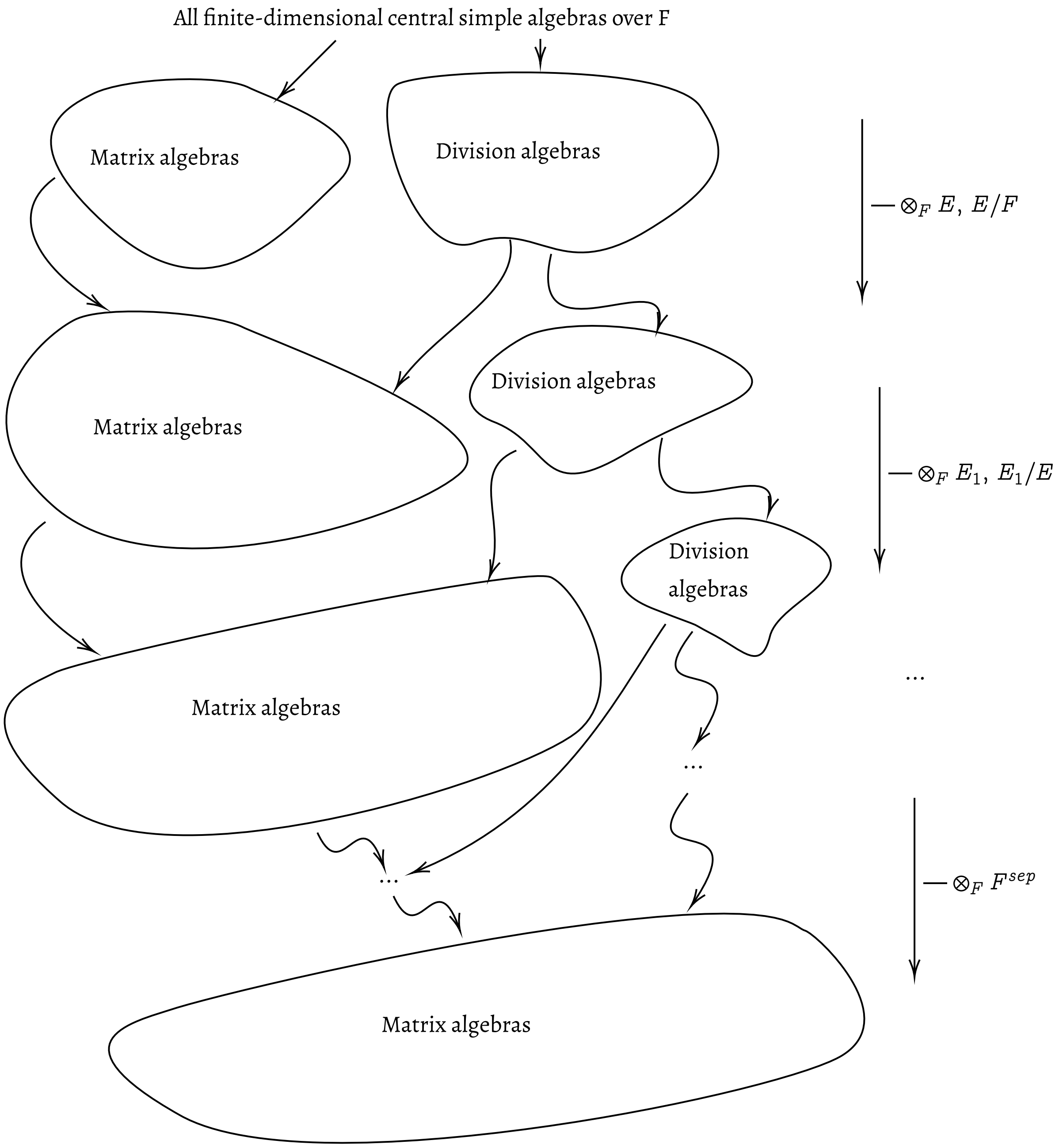

Figure 3.1: Algebras while extending scalars

3.2 Examples of central simple algebras

1. Any field F is a central simple F-algebra. It's a division algebra, $\dim_F F = 1$.
2. Hamiltonian quaternions $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$. Division algebra, $\dim_{\mathbb{R}} \mathbb{H} = 4$: $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$.
3. Another quaternion algebra over $\mathbb{R}$: $\left(\frac{1,-1}{\mathbb{R}}\right)$. Full matrix algebra of dimension 4.
4. Generalized quaternions:

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

Hamiltonian quaternions are a certain case when $a = b = -1$ and $F = \mathbb{R}$.

Whether a generalized quaternion algebra is matrix algebra or division algebra depends on a and b. For their classification we need to answer:

1. When two algebras with different a and b are isomorphic or not?

2. Is the given algebra a division algebra or full matrix algebra?

Quadratic forms will help us here.

Denote a generalized quaternion algebra $\left(\frac{a,b}{F}\right)$ by A. Then $A = F \oplus A_+$, where $A_+ = Fi \oplus Fj \oplus Fk$ — those are called *pure quaternions*. Define a norm on A: for element $x = c_0 + c_1 i + c_2 j + c_3 k \in A$ its conjugate is $x^* = c_0 - c_1 i - c_2 j - c_3 k$, and a norm is given by $v(x) = xx^* = c_0^2 - ac_1^2 - bc_2^2 + abc_3^2$ (see, adjunction and norm map are defined analogously with $\mathbb{C}$). When $c_0 = 0$, i.e. $x \in A_+$, we have $v(x) = -ac_1^2 - bc_2^2 + abc_3^2$. The following statements hold:

1. A — a division algebra $\iff$ the forms $c_0^2 - ac_1^2 - bc_2^2 + abc_3^2$ and $-ac_1^2 - bc_2^2 + abc_3^2$ are anisotropic, that is, they nullify only at zero,

2. A — a full matrix algebra $\iff$ $c_0^2 - ac_1^2 - bc_2^2 + abc_3^2$ and $-ac_1^2 - bc_2^2 + abc_3^2$ are isotropic, that is, nullify not only at zero.

One can analyze any of these forms or their equivalents. For exapmle, for $\mathbb{H}$ one sees that over $\mathbb{R}$ the form

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

can be zero only at 0, and hence $\mathbb{H}$ is a division algebra. It turns out that two quaternion algebras over field of characteristic non-equal to 2 are isomorphic $\iff$ the corresponding quadratic forms are equivalent (= there exists a non-trivial change of variables). In other words this statement is known as Witt's theorem, see [SC21, p. 8].

From this point of view there are only 2 quaternion algebras over $\mathbb{R}$:

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

This also plays a role in the fact that $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ (combined with Frobenius theorem).

A less trivial and yet more fascinating examples are quaternions over $\mathbb{Q}$. They are fully classified and there are several ideas and results which we'll give and discuss.

Theorem 3.2.1 (**Minkowski, Hasse**). *A quadratic form has a non-trivial zero over $\mathbb{Q}$ $\iff$ it has non-trivial zeros over $\mathbb{R}$ and $\mathbb{Q}_p$ for all prime p.*

Proof. [Ser96, p. 41] Q. E. D.

Theorem 3.2.2 (**Hensel's lemma**). *$f \in \mathbb{Z}_p[X]$ — a p-adic polynomial, $\alpha_0 \in \mathbb{Z}_p$ — a p-adic integer s.t. $f(\alpha_0) \equiv 0 \pmod{p^{2k+1}}$ and $f'(\alpha_0) \not\equiv 0 \pmod{p^{k+1}}$. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod{p^{k+1}}$.*

Proof. [Q G20, p. 89] Q. E. D.

This lemma is naturally generalized [1] to n variables:

Theorem 3.2.3. *$F(X_1, \ldots, X_n) \in \mathbb{Z}_p[X_1, \ldots, X_n]$ — a p-adic polynomial in n variables, and $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}_p^n$ such that $F(\gamma) \equiv 0 \pmod{p^{2k+1}}$ and for some $i = 1, \ldots, n$ we have $F'_{X_i}(\gamma) \not\equiv 0 \pmod{p^{k+1}}$. Then there exists $\alpha \in \mathbb{Z}_p^n$ such that $\alpha \equiv \gamma \pmod{p^{k+1}}$ and $F(\alpha) = 0$.*

Definition 3.2.1. *For $a, b \in \mathbb{Q}_p^\circ$ we define the **Hilbert symbol**:*

$$(a,b)_p = \begin{cases} 1, & ax^2 + by^2 - z^2 = 0 \textit{ has a non-trivial solution in } \mathbb{Q}_p, \\ -1, & \textit{otherwise.} \end{cases}$$

[1] Analogously, as fundamental theorem of algebra is generalized to polynomials in n variables.

Theorem 3.2.4. *a, b, c — coprime square-free integers. The equation*

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

has a non-trivial solution in $\mathbb{Q}$ $\iff$ all the following statements are true:

1. *a, b and c are not all positive nor all negative;*

2. *For any prime p which divides a, there exists such r that $b + r^2c \equiv 0 \pmod{p}$; same for b and c;*

3. *If a, b and c are all odd, then the sum of some two of them is divisible by 4;*

4. *If a is even, then $b + c$ or $a + b + c$ is divisible by 8; same for b and c.*

Proof. [Cas91, p. 20]. Peculiarly, as the athor notes at [Q G20, p. 107], condition 1 is not used in the proof and implied from conditions 2, 3 and 4. Q. E. D.

Theorem 3.2.5. *p — an odd prime number, a, b and c — coprime integers, not divisible by p. Then there exist integers x_0, y_0, z_0, not all divisible by p, such that*

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

Proof. [Q G20, p. 103] Q. E. D.

We'll also need the consequence:

Theorem 3.2.6. *p — an odd prime number, a, b and c — coprime integers, not divisible by p. Then*

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

has a non-trivial solution in $\mathbb{Q}_p$.

Proof. Apply Hensel's lemma to the previous theorem, see [Q G20, p. 105] Q. E. D.

Useful fact 3.2.1. *[Cas91, p. 21]*

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

where a, b, c — square-free integers, and x, y, z — arbitrary integers.

Discussion.

Based on the given information we'll provide 3 approaches to the classification of quaternions over rationals:

1. A direct usage of theorem 3.2.4;

2. The Hilbert symbol with theorem 3.2.6 (the point of this theorem is that it allows to make a classification using only a finite number of solution checks: we need to compute the Hilbert symbol for all odd primes which divide a and b. Interestingly, the check for 2 is not needed);

3. Useful fact 3.2.1 provides us with finding all the "basic" triples x, y, z (which give all the other solutions) by a mere bruteforce; thus it not only answers the question of presence of non-trivial solutions but actually finds them.

We point out that Hensel's lemma, apart from its usage for prooving some of the provided results, allows us to build approximate solutions just like the Newton's method does. This technique is called Hensel lifting. One also finds many other variations of Hensel's lemma. The usage of Hensel's lemma in deriving theorem 3.2.6 from theorem 3.2.5 lets us see how to, in theory, find integer solutions via it.

The gist of this theoretical method is that, first, we find a solution modulo p, then by Hensel's lemma we understand that this is a tail of an actual solution, and find its next part, now modulo p^2, and so on. Basing on the fact that integers are periodic in their p-adic writings, we, having found a potential period, check for being a solution the corresponding integer which gives such a periodic presentation. However, we won't use it, because bruteforce is easier.

If we programme in Wolfram Mathematica these 3 methods described above, all of them give, in result, one and the same picture:

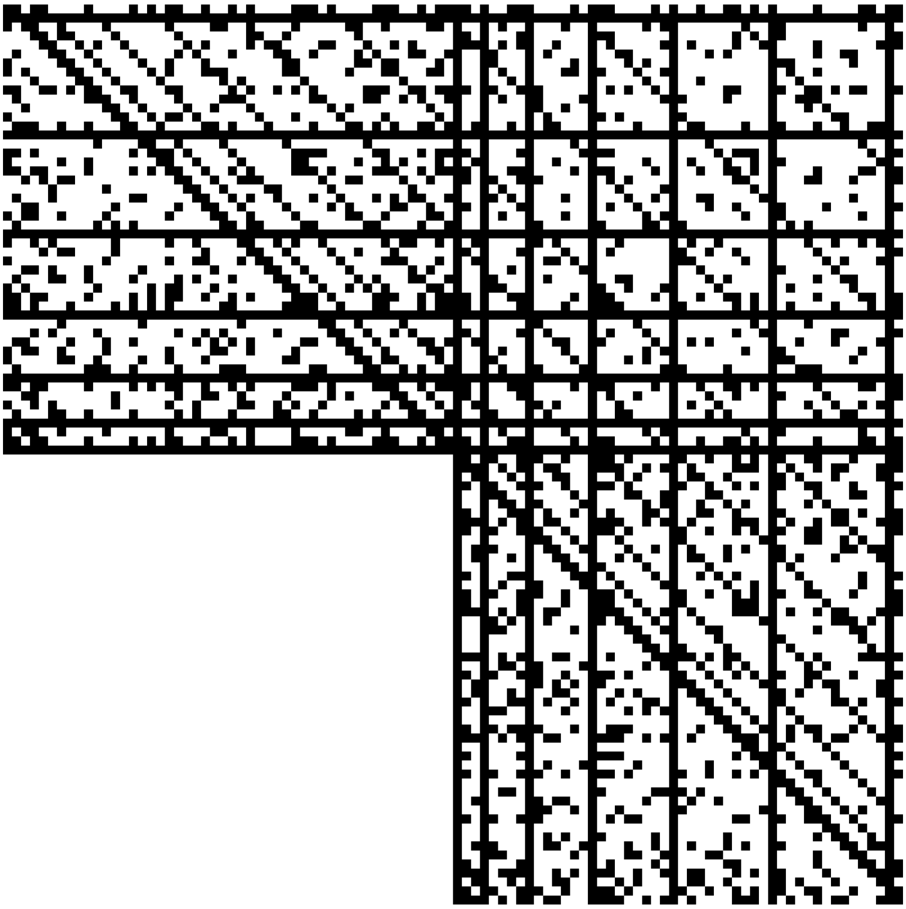

Figure 3.2: Quaternions over $\mathbb{Q}$ in range (-50, -49, ..., -1, 1, ..., 49, 50) for each axis. Black — one and the same $M_2(\mathbb{Q})$, white — possibly non-isomorphic division quaternion algebras over $\mathbb{Q}$.

Let's analyze the picture.

1. The white square in the 3rd quadrant: obviously, bacause a and b are negative;

2. The symmetry over "$y = x$": because of, for example, the equivalence of the forms $aX^2 + bY^2 - Z^2$ and $bX^2 + aY^2 - Z^2$;

3. The vertical and horizontal black lines: properties of quaternion algebras. $\left(\frac{a,1}{F}\right) \cong M_2(\mathbb{F})$ explains the black lines which border the big white squate. $\left(\frac{a,bc^2}{F}\right) \cong \left(\frac{a,b}{F}\right)$ justifies all the other vertical and horizontal black lines which emerge for a and b equal to 4, 9, 16, ...;

4. The first diagonal black line — $a + b = 0$ —..., $(-2, 2), (-1, 1), (1, -1), (2, -2)$, ...: quaternions' property $\left(\frac{a,-a}{F}\right) \cong M_2(F)$

5. The second diagonal black line — $a+b = 1$ — ..., $(-1, 2), (2, -1)$, ...: a property of the Hilbert symbol $(a, 1-a) = 1$. Note that the 1st quadrant's part of each black line is shifted down by 1 cell (compared to its prolongations) because 0 is dropped off.

6. The third diagonal black line — $a + b = 4$ — ... ,$(-1, 5)$, $(1, 3)$, $(2, 2)$, $(3, 1)$, ...; the fourth — $a + b = 9$, the fifth — $a + b = 16$ etc., where $a + b$ is a square. This can be explained by quadratic forms:

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

and the latter makes sense by the Hilbert symbol's property: $(a, 1 - a) = 1$.

From these explanations one can see that the languages of quadratic forms, of the Hilbert symbol and of properties of quaternion algebras are equivalent and it's possible to use any of them.

Let's take a look at a bigger picture:

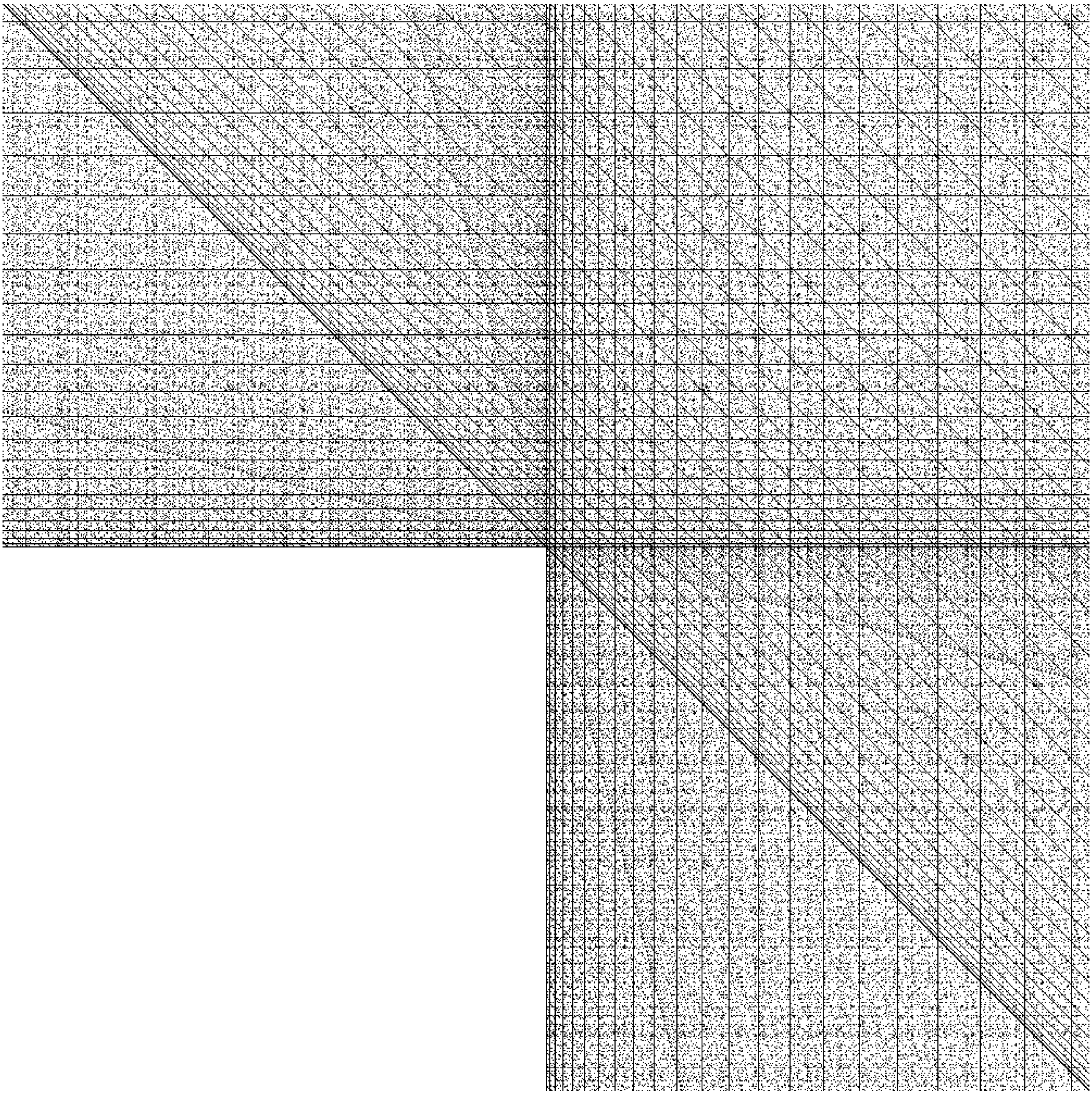

Figure 3.3: Quaternions over $\mathbb{Q}$ in range (-500, -499, ..., -1, 1, ..., 499, 500) for each axis. Black — one and the same $M_2(\mathbb{Q})$, white — possibly non-isomorphic division algebras over $\mathbb{Q}$.

On top of the patterns we've dealt with before we now can notice these four strange radial non-continious lines, two of them which are more consistent look like to be approximated by lines $y = -0.25x$ and $y = -4x$; the other two are less visible and more inclined to the line $y = -x$. What are they? Is this something new or not?

If we had not known some of the properties of math objects we'd talked of then we might could've found them by conjectures stated basing on the analysis of picture 3.2, provided that we hadn't used anything we "don't know" in writing the necessary algorithms. We'll use this backwards: exclude those pairs (a, b) which form the already known patterns. In this case if the radial lines go away, we'll conclude that they are just some combination of formulae we've seen before. If not, then we'll be to pose a conjecture on existence of something.

Having coloured such pairs' positions, where a or b is not square-free, we get

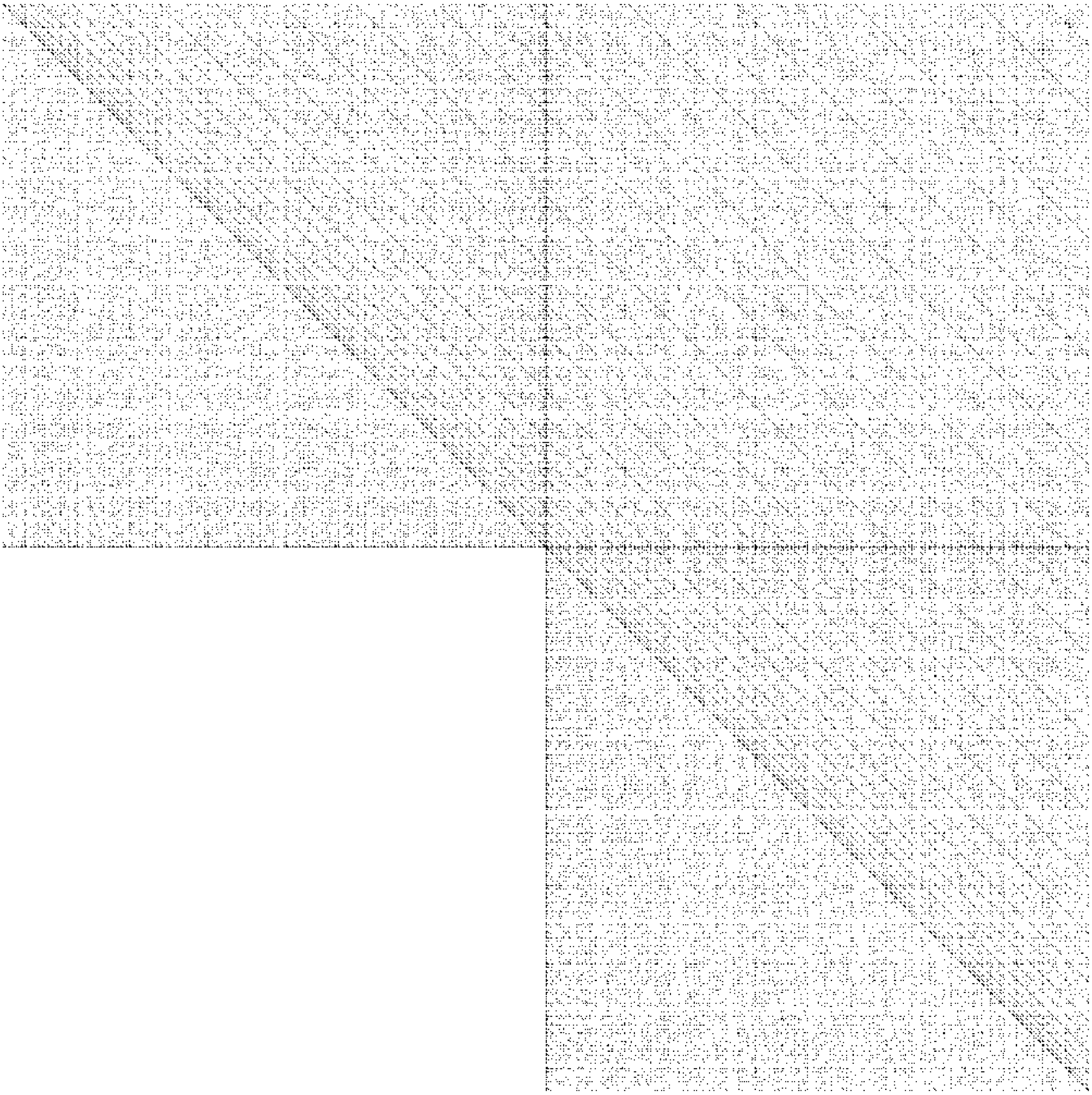

Figure 3.4: From -500 to 500, not square-free a and b pairs' squares are painted white as well as division algebras.

We see that that mysterious pattern goes away, hence the property of divisibility by squares is involved in its forming. After having painted white the other pairs which make familiar patterns, we get a uniform canvas:

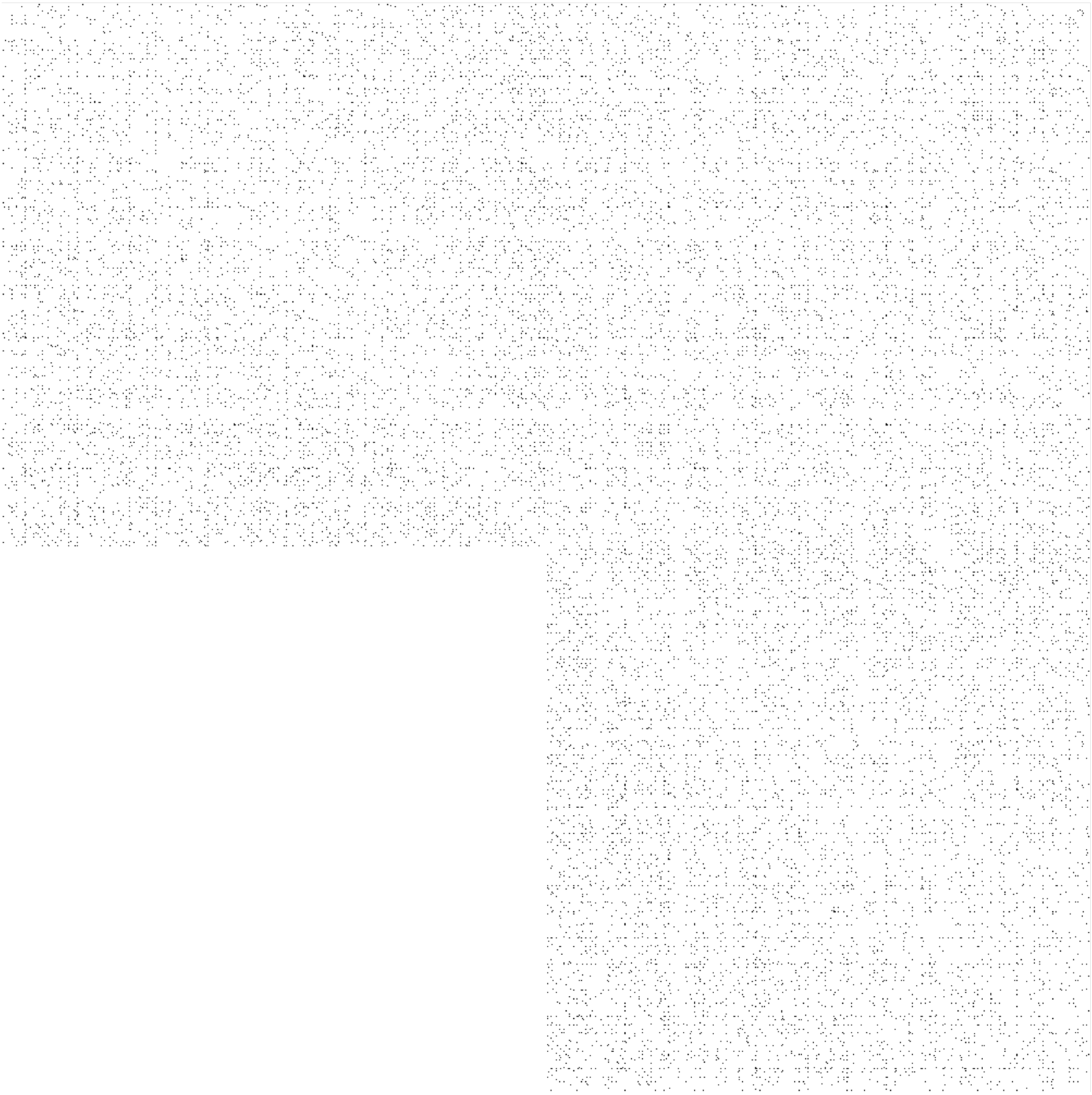

Figure 3.5: From -500 to 500, all understood pairs and/or division algebras are painted white.

This finishes the analysis of pictures. Note that one can use such a technique when solving an arbitrary problem: make some or other visualisation for stating a conjecture based on how do pictures change.

All the algorithms of classification along with picture generations and comments can be found in Appendix A, p. 50.

3.3 The Brauer group: classic approach

The Brauer group may mean two objects: the Brauer group of a field and the Brauer group of a scheme. We'll consider only the Brauer groups of fields.

The simplest invariant of an object which one can imagine is this object itself. Yet such invariants are not of much usage because they do not group different objects together by some shared properties.

The Brauer group is one of non-trivial field invariants which represent the information about field extensions and classes of central simple algebras. There are two approaches to describe the Brauer group of a field:

1. A natural one, based on considering the collection of all central simple algebras and on defining all the necessary structures; see [Pie82, p. 227]
2. By means of Galois cohomology which is less natural yet more handy in terms of working with the object; see [Pie82, p. 253]

Before giving the theory we'll give examples of some Brauer groups.

1. $\mathrm{Br}(\mathbb{F}_p) = 0$;
2. For any field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$, $\mathrm{Br}(\mathbb{F}_{p^n}) = 0$;
3. $\mathrm{Br}(\mathbb{C}) = 0$; in general, for any algebraically closed field F, $\mathrm{Br}(F) = 0$;
4. $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$;
5. For a local field F we have $\mathrm{Br}(F) = \mathbb{Q}/\mathbb{Z}$; examples of such fields are the field of p-dics $\mathbb{Q}_p$, and the field of Laurent series $\mathbb{F}_{p^n}((t))$;
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. $\mathrm{Br}(k) = 0$, if k is a field of type C_1, see [SC21, p. 14].

Recall our discussion of quaternions over $\mathbb{R}$: we had implicitly regarded that the dimensions of the algebras considered are ≤ 4; it turns out that there are no more algebras in a sense that we'll consider full matrix algebras to be equivalent, and for division algebras there is the following interesting result:

Theorem 3.3.1 (Frobenius). *Each finite-dimensional associative division algebra over $\mathbb{R}$ is isomorphic either to $\mathbb{R}$, or $\mathbb{C}$, or $\mathbb{H}$.*

Proof. See [BS19]; in this article one can find as a new elementary proof, so as the references to the old ones. Q. E. D.

It's peculiar that given an extra structure of Banach algebra we get a form of Gelfand-Mazur theorem: each non-trivial Banach algebra over $\mathbb{R}$ is isomorphic either to $\mathbb{R}$, or $\mathbb{C}$, or $\mathbb{H}$.

Frobenius theorem provides us with a description of the Brauer groups of reals and complexes. Nevertheless for local fields and for $\mathbb{Q}$ the situation is less trivial; we've seen quaternions over $\mathbb{Q}$ and they make us inclined to anticipate something complicated from the Brauer group of rationals. Indeed, class field theory is involved along with many exact sequences and alike. That's where we'll need an approach via Galois cohomology.

So, we'll give the required theory. Classic approach is the first.

Denote by $\mathfrak{S}(F)$ all central simple algebras over F.

Theorem 3.3.2. *Consider A, B from $\mathfrak{S}(F)$. The next conditions are equivalent:*

1. *There exists a division algebra $D \in \mathfrak{S}(F)$ and positive naturals n and m such that*
$$A \cong M_n(D) \text{ and } B \cong M_m(D);$$
2. *There exist positive naturals r and s such that $A \otimes M_r(F) \cong B \otimes M_s(F)$.*

Proof. [Pie82, p. 227] Q. E. D.

Based on that we have:

Definition 3.3.1. *Algebras A and B from $\mathfrak{S}(F)$ are called **equivalent** $\Longleftrightarrow$ they satisfy the conditions above. One writes $A \sim B$ in this case.*

The obtained factorset $\mathfrak{S}(F)/\sim$ is about to become our Brauer group. To this end we'll give a notion of the opposite algebra.

Definition 3.3.2. *The* ***opposite*** *(or the* ***adjoint****) of an R-algebra A is called an R-algebra A^{op}, which possesses the same structure of an R-module, as A does, yet with reversed multiplication: $x * y = yx$. Alternative writing: A^*.*

So,

Definition 3.3.3. *The* ***Brauer group*** *of a field F is a set $\{[A] : A \in \mathfrak{S}(F)\}$, with a group structure given by:*

1. $[A][B] = [A \otimes B]$ *— an operation;*
2. $[F]$ *— the identity;*
3. $[A]^{-1} = [A^*]$ *— the inverse element.*

Proof. Indeed, we need to show that the object defined is a group. See [Pie82, p. 228]. It's clear that (properties of $\otimes$) this group is abelian. Q. E. D.

The question arises: this group is abelian, however, we don't know yet how to compute it. It's not even clear what abelian groups are not Brauer groups of some fields. Actually, there is an open problem: for which natural n there exist a field F such that $|\mathrm{Br}(F)| = n$? [Aue+11, p. 31].

The prerequisites on abelian group classification we've given help us in understanding the Brauer group. It turns out that the Brauer group is a torsion group, that is, it's either a finitely generated group of the form $\mathbb{Z}/p_1^{k_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{k_n}\mathbb{Z}$, or a divisible group of the form $\bigoplus_p \left[\bigoplus_{r_p(D)} \mathbb{Z}(p^\infty)\right]$, or something unknown being a torsion subgroup in a group which is not finitely generated nor divisible. The fact the Brauer group is torsion may be proved without Galois cohomology, see [SC21, pp. 11–12]. With — [SC21, p. 22].

3.4 The Brauer group: Galois cohomology approach

Definition 3.4.1. *The* ***Brauer group*** *of a field F is*

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

where K^{sep} is a separable closure of K, and $(K^{sep})^\circ$ is a multiplicative group of K^{sep}.

There is an alternative description via the relative Brauer groups.

Definition 3.4.2. *The* ***relative Brauer group*** *of a Galois extension L/K is*

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

Definition 3.4.3. *The* ***Brauer group*** *of a field K is*

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

The description of this colimit is exactly as the one which first comes to mind. For detailed treatment see [Pie82, pp. 264–268].

Chapter 4

Group cohomology. The correspondence between Severi-Brauer varieties and central simple algebras. Amitsur's conjecture

4.1 Group cohomology with abelian and non-abelian coefficients

We'll consider the zeroth, the first and the second cohomology.

We won't need the higher cohomology of G*-modules* (H^i, $i \geq 3$); however, for $i = 3$ see [Bro82, p. 102], there are references for $i > 3$ as well which are formed by a mere generalisation: longer complexes are considered. The Brauer group is the main example of cohomology of G*-modules*, that is, it's cohomology with abelian coefficients.

Cohomology of G*-groups*, that is, non-abelian cohomology, we'll consider for dimensions 0 and 1. Defining cohomology of G*-groups* for $i \geq 2$ is problematic, see [Gir71] for the respective theory. The main example of cohomology of G*-groups* in our theory is the pointed set $\mathrm{H}^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathrm{PGL}_n(K^{\mathrm{sep}}))$.

Definition 4.1.1. *A — a Γ-set. Then*

$$\mathrm{H}^0(\Gamma, A) = A^\Gamma = \{a \in A \mid \sigma a = a \textit{ for all } \sigma \in \Gamma\}$$

In other words, zeroth cohomology are Γ-invariants. We point out the essential difference from cohomology in R-mod: in a long exact sequence in R-mod instead of $\mathrm{H}^0(\ldots)$ we write $\mathrm{Hom}(\ldots)$, whereas in this case we'll write A^Γ. This poses a question: is H^1 a right derived functor, likewise it's a derived functor in R-mod? The answer is yes, see [Mil22, p. 94]. More interestingly: is it possible to construct the higher cohomology of G-groups via derived functors?

The further definition of non-abelian cohomology is done via defining 1-cocycles and then factoring them by the equivalence to be defined as well.

Definition 4.1.2. *A — a Γ-group. Then a* ***1-cocycle*** *in Γ with a value in A is called a continious map $\alpha\colon \Gamma \to A$ such that*

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

The set of all these 1-cocycles is denoted by $Z^1(\Gamma, A)$. A map which sends everything to the unity, $\alpha(\sigma) = 1$ for all $\sigma \in \Gamma$, is the basepoint in this pointed set.

Two 1-cocycles $\alpha, \beta \in Z^1(\Gamma, A)$ are called equivalent (or ***cohomologous****) $\iff$ there exist $a \in A$, such that*

$$\beta(\sigma) = a \cdot \alpha(\sigma) \cdot \sigma a^{-1} \textit{ for all } \sigma \in \Gamma.$$

[1] Crossed homomorphism here is in multiplicative notation, since A — a Γ-group, not a Γ-module, that is, commutativity is not assumed.

Having denoted this equivalence by $\sim$, we define

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

Note that *if* A is a Γ-module, then $Z^1(\Gamma, A)$ is an abelian group with the induced operation $(\alpha\beta)(\sigma) = \alpha(\sigma)\beta(\sigma)$, and, therefore, $\mathrm{H}^1(\Gamma, A)$ is abelian, too; since the sum/difference of crossed homomorphisms is again a crossed homomorphism, and since the sum/difference of principal crossed homomorphisms is a principal crossed homomorphism, then $\mathrm{H}^1(\Gamma, A)$ admits the following alternative definition.

Definition 4.1.3. *A — a Γ-module. Then*

$$\mathrm{H}^1(\Gamma, A) = \frac{\textit{crossed homomorphisms from } \Gamma \textit{ to } A}{\textit{principal crossed homomorphisms from } \Gamma \textit{ to } A}$$

Note that in the case of Γ-modules the difference of crossed homomorphisms which is a principal crossed homomorphism is compatible with equivalence we've given for Γ-groups. Indeed, in the multiplicative form we have

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

for some $a \in A$. Then

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

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

We point out that for the definition of 1-cocycles we've used the variant ••[2], however, the variant • is more natural because it's compatible with a hypothetical group structure on $\mathrm{H}^1(\Gamma, A)$. This nuance will come up further, since there is the question: what is an obstacle for defining a group structure on $\mathrm{H}^1(\Gamma, A)$ when A is a Γ-group? The matter is that in abelian case we had the ability to induce the operation on $Z^1(\Gamma, A)$ by $(\alpha\beta)(\sigma) = \alpha(\sigma)\beta(\sigma)$ without facing any obstacles because having considered the next two manipulations with parentheses

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

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

we see, that condition *=** gives no restrictions because of the commutativity of A. Hence, only a subset of 1-cocycles $\alpha \in Z^1(\Gamma, A)$, where A is a Γ-group, such that

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

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

can be provided with a group structure induced from A. Then a natural desire is to obtain from this group a normal subgroup of principal crossed homomorphisms. This is here where we'll need, in particular, • for describing the arising factorgroups. However, we'll omit the detailed discussion of this matter for the future times.

Definition 4.1.4. *A is a Γ-module. A* ***2-cocycle*** *from Γ to A is a continious map $\alpha\colon \Gamma \times \Gamma \to A$ such that*

$$\sigma\alpha(\tau, \rho) \cdot \alpha(\sigma, \tau\rho) = \alpha(\sigma\tau, \rho)\alpha(\sigma, \tau) \textit{ for all } \sigma, \tau, \rho \in \Gamma.$$

The set of all 2-cocycles from Γ to A is denoted by $Z^2(\Gamma, A)$. This set is an abelian group:

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

[2] The same variant is used in [Jah03, p. 5] and [Knu+98, p. 384].

*Two 2-cocycles α u β are called equivalent (or **cohomologous**) $\iff$ there exists a continious map $\varphi\colon \Gamma \to A$ such that*

$$\beta(\sigma,\tau) = \sigma\varphi(\tau)\cdot\varphi^{-1}(\sigma\tau)\cdot\varphi(\sigma)\cdot\alpha(\sigma,\tau) \textit{ for all } \sigma,\tau\in\Gamma.$$

Having denoted this equivalence by $\sim$, we define

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

An example of this definition is the Brauer group. There is the following result: if A is a Γ-module, then $\mathrm{H}^2(\Gamma,A)$ is a set of equivalence classes of extensions of Γ by A (with respect to the action of Γ on A). The group operation on this set is called the *Baer sum*, where zero corresponds to the splitting extension, see, for example, [Wei94, p. 78]. In [Wei94, p. 79] there is an account on a natural generalisation of cohomology of Γ-modules for $i\geq 3$. Also, see [Rot08, p. 428].

Now we'll discuss the short exact sequences we have. For cohomology in R-mod a long exact sequence arises from the Snake lemma; for G-mod there is an analogous exact sequence with a connecting homomorphism. We start with considering $A\to B\to B/A$.

If B is a Γ-group, and A is a Γ-subgroup in B, then $B/A = \{b\cdot A \mid b\in B\}$ is a Γ-set. The map $B\to B/A$ induces $B^\Gamma \to (B/A)^\Gamma$. Further, $b\cdot A\in(B/A)^\Gamma \iff \sigma b\cdot A = b\cdot A$ for all $\sigma\in\Gamma$. The class of 1-cocycle $\alpha\colon\Gamma\to A$, which is defined as $\alpha(\sigma) = b^{-1}\cdot\sigma b\in A$, $[\alpha]\in\mathrm{H}^1(\Gamma,A)$, does not depend on b and hence there is the following map of pointed sets:

$$\delta^0\colon (B/A)^\Gamma \to \mathrm{H}^1(\Gamma,A),$$
$$b\cdot A\mapsto[\alpha],$$
$$\alpha(\sigma) = b^{-1}\cdot\sigma b.$$

Finally,

Theorem 4.1.1. *The sequence*

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

is exact.

Proof. The exactness at $(B/A)^\Gamma$: assume that 1-cocycle $b^{-1}\cdot\sigma b\in A$ is trivial at $\mathrm{H}^1(\Gamma,A)$, that is, $\alpha(\sigma) = a^{-1}\cdot\sigma a$ for some $a\in A$. Then $ba^{-1}\in B^\Gamma$ and $b\cdot A = ba^{-1}\cdot A$ в B/A is the image of $ba^{-1}\in B^\Gamma$.

The exactness at $\mathrm{H}^1(\Gamma,A)$: if $\alpha\in Z^1(\Gamma,A)$, $\alpha(\sigma) = b^{-1}\cdot\sigma b$ for some $b\in B$, then $b\cdot A\in(B/A)^\Gamma$ and $[\alpha] = \delta^0(b\cdot A)$. The exactness at other terms is clear. Q. E. D.

A longer sequence:

Theorem 4.1.2. *B — a Γ-group, A — a Γ-subgroup in B, and $C = A/B$ (a Γ-group, too). Then the sequence*

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

is exact.

Proof. Exactness at $\mathrm{H}^1(\Gamma,B)$: take $\beta\in Z^1(\Gamma,B)$ such that $[\beta]$ lies in the kernel of the latter map in the chain. Then

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

for some $b\in B$. Thus,

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

for $\alpha\in Z^1(\Gamma,A)$, and $[\beta]$ — the image of $[\alpha]$ in $\mathrm{H}^1(\Gamma,B)$. The exactness of other terms is proved by the previous theorem. Q. E. D.

Finally, if B — a Γ-group, A — a *central* Γ-subgroup in B, then A — an abelian group and the connecting homomorphism

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

is defined as follows. For $\gamma \in Z^1(\Gamma, C)$ choose $\beta\colon \Gamma \to B$ such that $\beta(\sigma)$ is mapped to $\gamma(\sigma)$ for all $\sigma \in \Gamma$. Consider a map $\alpha\colon \Gamma \times \Gamma \to A$, defined as

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

$\alpha \in Z^2(\Gamma, A)$ and the corresponding equivalence class does not depend on the choice of $\gamma \in [\gamma]$ and β. Thus,

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

Then,

Theorem 4.1.3. *The sequence*

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

is exact.

Proof. The exactness at $\mathrm{H}^1(\Gamma, C)$: consider $\gamma \in Z^1(\Gamma, C)$ and β, α such as described above. Then

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

for some $a(\sigma) \in A$. Then 1-cocycle $\beta(\sigma) \cdot a(\sigma)^{-1} \in Z^1(\Gamma, B)$, and its image — γ. The exactness at other terms is proven above. Q. E. D.

These results will be used later.

4.2 Key auxiliary theorems

Theorem 4.2.1 (Skolem, Noether). *R — a commutative ring with unity. Then $\mathrm{GL}_n(R)$ acts on $\mathrm{M}_n(R)$ by conjugation:*

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

If R — a field, then there is an isomorphism

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

Proof. [Jah03, p. 19], [SC21, pp. 20–21], [Pie82, pp. 230–231]. Q. E. D.

In other words, all the automorphisms of central simple algebra over field are inner. The direct usage of this theorem is a proof of the next one.[3]

Theorem 4.2.2 (Hilbert's theorem 90). *L/K — a Galois extension with Galois group G. Then*

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

Proof. [Knu+98, p. 393]. See also [Pie82, p. 312] for the original formulation of this theorem. Q. E. D.

The main yet not unique usage of this theorem is as follows. From the short exact sequence

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

the long exact sequence arises:

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

and by Hilbert's theorem 90 we have $\mathrm{H}^1(G, \mathrm{GL}_n(K)) = 0$, hence, the latter map between the familiar objects (for which G — an absolute Galois group) has trivial kernel.

[3] From the other hand, in [SC21, pp. 20–21] the situation is inverse: Hilbert's theorem 90 is used to prove the Skolem-Noether theorem.

4.3 Severi-Brauer varieties

Severi-Brauer varieties can be defined in several ways. We've seen one of them on the example of quaternion algebras: the corresponding form is given by the norm.

Definition 4.3.1. *The* ***Severi-Brauer variety*** *is a form of projective space. More precisely: n — a natural number; the* ***Severi-Brauer variety*** *of dimension $n-1$ over field K is a twisted form of projective space P_K^{n-1}.*

The problem with defining Severi-Brauer varieties is that they require a lot of equations. One of the ways to define them can be found in [Jac96, pp. 111–113] and this way is a very tedious approach with lots of formulae with towers of indeces. There also one finds an example of Severi-Brauer variety of quaternion algebra which is given by 31 equations. On top of that there is an article [Gar20] which provides 2 ways to define SB varieties, along with examples.

The first way provides an enormous amount of equations, once again; when computing these equations, the most complex task is to find a matrix of isomorphism $\varphi \in \mathrm{GL}_{m+1}(\overline{K})$ from lemma 5.1, [Gar20, p. 5]. Despite the fact that central simple algebras being considered are cyclic, still it's hard to find this matrix in a general form using Hilbert's theorem 90, because of the symbolic computations: the determinant of 10 by 10 matrix which elements are *symbolic* linear combinations is involved. In fact, in this lemma 5.1 the proper matrix is only given, yet no detailed account on how to get it is given. Besides, there is a question of finding such φ that the resulting equations will be in their simplest form. Also note that Veronese equations can be obtained much easier then in the article (proposition 3.4 in it), namely, mere by 2 by 2 minors of symmetric matrix of variables.

The second approach gives *one* equation using norms, see [Gar20, p. 9]. See also [Jac96, p. 138].

4.4 Theorems on correspondence

Theorem 4.4.1. *L/K — a finite Galois extension, $G = \mathrm{Gal}(L/K)$ — the corresponding Galois group, n — a natural number. Then there exists a bijection of pointed sets:*

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

$$A \mapsto a_A.$$

Proof. [Jah03, p. 20] Q. E. D.

Theorem 4.4.2. *L/K — a finite Galois extension, $G = \mathrm{Gal}(L/K)$ — the corresponding Galois group, n — a natural number. Then there exists a bijection of pointed sets:*

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

$$X \mapsto \alpha_X.$$

Proof. [Jah03, p. 24] Q. E. D.

These two theorems are combined into one which describes the correspondence between Severi-Brauer varieties and central simple algebras.

Theorem 4.4.3. *n — a natural number, K — a field, A — a central simple algebra of dimension n^2 over K. Then:*

1. *There exists a Severi-Brauer variety X_A of dimension $n-1$ over K, such that the following holds: if L/K — a finite Galois extension splitting A, then it splits X_A as well, and there is one and the same class*

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

   corresponding to A and X_A. This condition defines X_A up to isomorphism of K-schemes.

2. *For the correspondence $X \colon A \mapsto X_A$ we have:*

(a) *X is compatible with extensions K'/K of the base field:*

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

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

Proof. [Jah03, p. 29] Q. E. D.

The next theorem is of interest for it reflects the phenomenon we've seen on the example of quaternions: the existing of a non-trivial solution, a point, means that we've faced a matrix algebra — yet in geometrical terms.

Theorem 4.4.4. *r — a natural number, X — a Severi-Brauer variety of dimension r over K, $X(K) \neq \emptyset$. Then*

$$X \cong P_K^r.$$

Proof. [Jah03, pp. 26–27]. We point out that Hilbert's theorem 90 is used here for the proof, too. Q. E. D.

Besides, the above mentioned way of defining Severi-Brauer varieties also gives a description of the correspondence between Severi-Brauer varieties and central simple algebras, and allows us to obtain the equations of a Severi-Brauer variety from the corresponding central simple algebra; see [Jac96, pp. 107–114].

4.5 Possible ways to solve the Amitsur's conjecture

As we've discussed earlier in the introduction, Amitsur in his work [Ami55] had obtained the following result:

Theorem 4.5.1. *Two Severi-Brauer varieties are birationally isomorphic $\implies$ the corresponding central simple algebras have the same degree and their classes generate the same cyclic subgroup in the Brauer group.*

The conjecture is: the inverse implication holds. The results on this conjecture as well as the theory around it may be found in [Ami55], [Roq64], [Tpe91], [Kra02], [Flo10], [Nov16], [Mat20].

There are opinions which I've gained from the direct conversations with people who work in this topic that, actually, this conjecture is false in general and there might be some sophisticated counterexample. However, who and when could've been stopped by this?

The following strategies of solving the Amitsur's conjecture which may have sense have come up in my mind.

Building chains of invariants

Birational varieties are, actually, non-isomorphic. However, this is an equivalence. There are many equivalences and any two objects are natural to compare up to some equivalence; based on that fact there is the following strategy. Given two Severi-Brauer varieties the fact of equivalence of which initially is not known, we build two objects invariants corresponding to them and these objects are designed so that some equivalence of them would imply (or implied by, or equivalent to) the equivalence of the initial objects, that is, of Severi-Brauer varieties. If this is not enough, then we build the second objects invariants of the first objects invariants with an equivalence which would again either imply, or be implied by, or be equivalent to the equivalence of the first, lower objects. There may be even a set of such equivalences, each paired with $\implies$, $\impliedby$ or $\iff$ with respect to some of the equivalences of the preceding objects. And so on. This chain of invariants along with equivalences can in a sense be regarded as a collection of zooming lenses or as a microscope which helps us to distinguish two initial objects. Hence, the chain should be built such that it would help us with the initial classification problem. Clearly this strategy can be applied to any objects in general, not just Severi-Brauer varieties. Actually, all mathematical problems can be regarded as problems of classification: mathematics is full of computations, rewritings, and all of them do classify things, don't they? The model of vision of mathematics in which it's split to classification problems and problems of building tools for classification seems making sense to me; of course these problems do not exclude each other, they are like yin and yang.

To conclude, the question of building such chains of invariants is how to decode all the necessary information the initial object possess, how to detach it and present it fully in the upper objects so that the method could work. Besides, such chains may have a functorial sense.

The finiteness of the Brauer group

This hypothetical method is based on the following. First, set the case when the Brauer group is finite. Second, since the first cohomology pointed set is included into the Brauer group, we explicitly build for each element of this pointed set (perhaps, via some computational packages like Wolfram Mathematica) the corresponding Severi-Brauer variety (it's equations) and the central simple algebra. Last, we try to analyse the behaviour of the classes in the Brauer group, namely, whether they generate the same cyclic subgroup or not; and how does it relate to the degree of the respective central simple algebras, and so on. However, the entire case analysis is problematic because the finiteness of the Brauer group is still an open problem and is connected with another open problem, namely, Tate-Shafarevich conjecture on the finiteness of the Tate-Shafarevich group. It's known that the finiteness of the Brauer group is equivalent to the finiteness of the Tate-Shafarevich group when certain conditions are satisfied, see Proposition 4.5, [Gro68, p. 118]. See also [SC21, p. 395]. Perhaps, the analysis of Amitsur's conjecture in the case of equivalence of the Brauer group and the Tate-Shafarevich group would yiled something new.

Conclusion

The main result of this work is the work itself, which appears to be a detailed survey on the theory of Severi-Brauer varieties and central simple algebras. During the research on this topic I was aiming to capture the readers interest with a non-stiff language, with examples, questions, and the needed references — all with the question "who's going to read this?" in mind. As for those people unfamiliar with the subject, I believe, the work in general and quaternions in particular are of interest; as for those who is somehow or other related to the subject, various questions along the work and two strategies of solving Amitsur's conjecture, I reckon, should be of mathematical interest.

That is, the goals are reached and there still is a potential for the work to come, namely, in the research in theory of central simple algebras and Severi-Brauer varieties.

Books

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

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

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

[BO13] G. Berhuy and F. Oggier. *An introduction to central simple algebras and their applications to wireless communication*. 2013.

[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 et al. *The Book of Involutions*. AMS, 1998.

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

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

[LS09] F. William Lawvere and 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*. 2nd ed. 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, and 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 and 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 and 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 and К. А. Шрамов. *Неразветвлённая группа Брауэра и её приложения*. МЦНМО, 2018.

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

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

Articles, surveys, notes and other

[Ami55] S. A. Amitsur. "Generic Splitting Fields of Central Simple Algebras". In: *Ann. Math* 62 (1955), pp. 8–43.

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

[BS19] Matej Brešar and 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". In: *Doc. Math.* 8 (2002), pp. 527–546.

[Kra08] D. Krashen. "Birational maps between generalized Severi-Brauer varieties". In: *Pure Appl. Alg.* 212 (2008), pp. 689–703.

[Mat20] E. Matzri. "A birational interpretation of Severi-Brauer varieties". In: *Communications in Algebra* 48 (2020), pp. 484–489.

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

[Roq63] P. Roquette. "On the Galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras". In: *Math. Ann.* 150 (1963), pp. 411–439.

[Roq64] P. Roquette. "Isomorphisms of generic splitting fields of simple algebras". In: *Reine Angew. Math.* 214/215 (1964), pp. 207–226.

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

[Wit34] E. Witt. "Über ein Gegenbeispiel zum Normensatz". In: *Math. Z.* 39 (1934), pp. 462–467.

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

[Тре91] С. Л. Трегуб. "О бирациональной эквивалентности многообразий Брауэра-Севери". In: *Russ. Math. Surv.* 46.6 (1991), p. 229.

Appendix A

Wolfram Language code for classification of quaternions and finding integer solutions

See the next page.

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=±p_1^{α_1}...p_n^{α_n}, alpha[a,p_i]=α_i *)
```

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:

$|a|\,x^2 + |b|\,y^2 + |c|\,z^2 \leq 4\,|\text{abc}|$

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

$|a|\,x \leq 4\,|\text{abc}|$

$x \leq 4\,|\text{bc}|$

$x \leq 2\left\lfloor\sqrt{|b\,c|}\right\rfloor$

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
```