Список литературы

1. *Абрамов А.*. Введение в тензорный анализ и риманову геометрию. М., 2012.
2. *Акивис М.А.* Многомерная дифференциальная геометрия. Калинин, 1977.
3. *Катанаев М.О.* Геометрические методы в математической физике : курс лекций. 2015.
4. *Лаптев Г.Ф.* Основные инфинитезимальные структуры высших порядков на гладком многообразии // Тр. геом. семин. ВИНИТИ. М., 1966. Т. 1. С. 139—189.
5. *Остиану Н.М.* Геометрических объектов теория // Мат. энц. М., 1984. Т. 1. С. 937.
6. *Полякова К.В.* Параллельные перенесения направлений вдоль поверхности проективного пространства // Дифференциальная геометрия многообразий фигур. Калининград, 1996. Вып. 27. С. 63—70.
7. *Рашевский П.К.* Риманова геометрия и тензорный анализ. М., 1967.
8. *Рыбников А.К.* Об аффинных связностях второго порядка // Матем. заметки. 1981. Т. 29, вып. 2. С. 279—290.
9. *Чакмазян А.В.* Нормальная связность в геометрии оснащенных подмногообразий аффинного пространства // Итоги науки и техн. Сер.: Пробл. геом. 1989. Т. 21. С. 93—107.
10. *Шевченко Ю.И.* Оснащения голономного и неголономного гладких многообразий. Калининград, 1998.

Об авторе

Катерина Валентиновна Полякова — канд. физ.-мат. наук, доц., Балтийский федеральный университет им. И. Канта, Калининград.
E-mail: polyakova_@mail.ru

About author

Dr Katerina Polyakova — Ass. Prof., I. Kant Baltic Federal University, Kaliningrad.
E-mail: polyakova_@mail.ru

УДК 512.742.2

А.А. Смирнов

ОБЗОР СУЩЕСТВУЮЩИХ ОБОБЩЕНИЙ ТЕОРЕМЫ ДОЙРИНГА О РЕДУКЦИИ

Исследуются различные обобщения теоремы Дойринга о редукции. Выясняется, что наиболее подходящей для дальнейшего уточнения является теорема, связывающая разложение $p\square_K$ на простые идеалы с разложением $A[p]$ на неразложимые BT_1-групповые схемы с точностью до изоморфизма. Определяются основные проблемы дальнейшего обобщения теоремы, некоторые пути их решения и ставятся задачи для последующей работы в этом направлении.

Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2016. № 4. С. 10 – 15.

The article is focused on various generalizations of the Deuring Reduction Theorem. Our research proves that the most appropriate theorem for further elaboration is the one that relates the decomposition of $p\mathcal{O}_K$ into prime ideals with the decomposition of $A[p]$ into indecomposable BT_1-group schemes up to isomorphism. The article investigates basic problems of the theorem's further generalization and some ways of solving them as well as formulates tasks for further work in this direction.

Ключевые слова: абелевы многообразия, точки p-кручения, теорема Дойринга, BT_1-групповые схемы, круговые слова.

Key words: abelian varieties, p-torsion points, Deuring Reduction Theorem, BT_1-group schemes, circular words.

Введение

Одним из важнейших атрибутов любого абелева многообразия A размерности g являются его точки p-кручения, которые образуют конечную группу $A[p]$. Ее порядок равен p^{2g}, кроме случая, когда многообразие определено над алгебраически замкнутым полем k характеристики p — тогда порядок группы $A[p]$ не будет превосходить p^g.

На сегодня существуют различные способы описать точки p-кручения, однако менее исследованным остается вопрос о том, как по конкретному идеалу $\mathfrak{P}$, в котором многообразие имеет хорошую редукцию, вычислить группу $A[p]$, где $p = \mathfrak{P} \cap \mathbb{Z}$.

В случае, когда $g = 1$, ответ на этот вопрос дает теорема Дойринга о редукции. В терминах групповых схем ее можно сформулировать следующим образом.

Теорема. *Пусть $\mathcal{E}$ — эллиптическая кривая над числовым полем, обладающая комплексным умножением на $\mathcal{O}_K$ — порядок в мнимом квадратичном поле K. Пусть $\mathfrak{P}$ — идеал в $\overline{\mathbb{Q}}$, лежащий над простым числом p, в котором $\mathcal{E}$ имеет невырожденную редукцию E. Тогда*

$$E[p] \times \overline{\mathbb{F}}_p \cong \begin{cases} \mathrm{I}_{1,1}, & \text{если } p\mathcal{O}_K = \mathfrak{P}^2 \text{ или } p\mathcal{O}_K = \mathfrak{P}, \\ \mathbb{Z}/p\mathbb{Z} \times \mu_p, & \text{если } p\mathcal{O}_K = \mathfrak{P}\overline{\mathfrak{P}}. \end{cases}$$

Для абелевых многообразий размерности 2 и 3 существует обобщение данной теоремы, описанное в статье [21]. В связи с этим возникает вопрос: можем ли мы для абелева многообразия произвольной размерности, обладающего комплексным умножением на $\mathcal{O}_K$, найти способ связать разложение групповой схемы $A[p]$ на компоненты с разложением идеала (p) в кольце $\mathcal{O}_K$? Существует ли общая теорема, описывающая подобную связь? Если нет, то можем ли мы описать общий алгоритм, который позволит вычислять на компьютере зависимости между разложениями для данного $g \geqslant 1$?

1. Обзор результатов

Особую роль в изучении абелевых многообразий играют точки конечного порядка. Известно, что группа точек p-кручения абелева многообразия $A_{/k}$ размерности g изоморфна группе $(\mathbb{Z}/p\mathbb{Z})^f$, где k — алгебраически замкнутое поле характеристики p. Число f в этом случае называется p-рангом многообразия A. Если $f = g$, то многообразие называется обыкновенным, а в другом крайнем случае, при $f = 0$, — суперсингулярным.

Суперсингулярные абелевы многообразия представляют особый интерес, в частности, для криптографии. Их изучению посвящено множество работ, среди которых можно отметить [1; 8; 20]. Ясно, что теорема Дойринга, среди прочего, дает ответ на вопрос, как свойство суперсингулярности многообразия зависит от разложения идеала (p).

В исследовании точек p-кручения немаловажен вопрос об их количестве, когда абелево многообразие рассматривается над некоторым фиксированным числовым или p-адическим полем K. Задача состоит в том, чтобы ограничить сверху число элементов множества $A(K)[p]$ некоторой функцией $F(K)$. Описание подобных границ для числа точек можно найти, например, в статьях [4; 5; 19]. Также вопрос о конечности $A(K)[p]$ исследовался еще Рибетом в работе [17]. Возможно, что некоторые новые результаты в этом направлении удастся получить, если учесть специфику структуры $A(\overline{\mathbb{F}}_p)[p]$ как конечной групповой схемы.

Различные способы описания точек p-кручения абелевых многообразий описаны в [16]. Автор статьи выделяет основные типы классификации точек p-кручения, а также дает описание группы $A[p]$ главнополяризованного абелева многообразия произвольной размерности g для некоторых важных частных случаев. Кроме того, в конце статьи приводятся таблицы всевозможных типов точек p-кручения, возникающих при $g \leqslant 4$. Заметим, что для $g \leqslant 3$ данный результат полностью перекрывается главной теоремой статьи [21].

Описывая точки p-кручения как квазиполяризованные BT_1-групповые схемы ранга p^{2g}, мы можем их классифицировать благодаря работам [12; 13; 15]. В свою очередь, для классификации BT_1-групповых схем, существуют различные комбинаторные методы, которые можно найти в [9; 15]. Если же подходить к вопросу о классификации точек p-кручения, используя теорию ковариантных Дьёдонне модулей, то обратиться можно к результатам, описанным в [6; 11]. Однако данные описания лишь дают представление о том, какими могут быть точки p-кручения, но не о том, в каких случаях они возникают.

Наконец, зависимость между $A[p]$ и разложением $p\mathcal{O}_K$ на простые идеалы была прослежена в статье [10], но лишь для случая абелевых поверхностей, то есть при $g = 2$. В [18] эта зависимость также отразилась в некоторых частных результатах, которые местами пересекаются с основной теоремой статьи [21], однако не обладают той же полнотой, поскольку там описаны лишь некоторые определенные типы разложения

идеала $p\mathcal{O}_K$, благодаря чему все доказательства приведены для произвольной размерности многообразия. Кроме того, в [3] описана явная связь между разложением $p\mathcal{O}_K$ и p-рангом многообразия A, что полностью покрыто результатами работы [21]. Стоит также упомянуть результат Блэйка [2], который, хоть и не дает явных результатов, но приводит общую теорему, дающую полное обобщение теоремы Дойринга для абелевых многообразий произвольной размерности. Тем не менее Блэйк формулирует теорему в терминах многоугольников Ньютона, благодаря которым групповую схему $A[p]$ можно восстановить лишь с точностью до изогении, но не изоморфизма, как в статье [21]. В связи с этим хотелось бы обобщить теорему Дойринга именно в духе статьи [21] таким образом, чтобы научиться по разложению идеала (p) определять все возможные соответствующие этому разложению неизоморфные групповые схемы $A[p]$.

2. Проблемы и возможные пути решения

1. Общий алгоритм. В оригинальной статье [21] алгоритм построения соответствий между разложениями идеала $p\mathcal{O}_K$ и разложениями групповой схемы $A[p]$ приведен в неявном виде, последовательность действий можно проследить лишь на примерах с конкретными группами Галуа и не всегда очевидно как следует поступать в общей ситуации, когда заведомо не известна специфика той или иной группы. Более того, алгоритм потребует некоторых оптимизаций, поскольку в основе своей он имеет обыкновенный перебор всех возможных случаев, поэтому стоит ожидать, что сложность будет быстро расти с ростом размерности. К примеру, в размерности 3 существует 4 неизоморфных группы, подходящих на роль группы Галуа $G = \mathrm{Gal}(\hat{K}/\mathbb{Q})$, где $\hat{K}$ — замыкание Галуа СМ-поля K. В размерности 4, как показано Додсоном в статье [7], таких групп уже 30, и к каждой из них нужно применить весь алгоритм, чтобы получить полный результат. Предполагаемый порядок действий: формализовать алгоритм из статьи [21], реализовать его в системе компьютерной алгебры GAP и оптимизировать его работу, пока не будут получены результаты, по крайней мере для тех входных данных, которые заранее известны благодаря статьям [7; 21].

2. Входные данные. Общий алгоритм потребует на вход два параметра: размерность абелева многообразия g и список всевозможных групп G, возникающих как группы Галуа для замыканий Галуа всевозможных СМ-полей размерности $2g$ над $\mathbb{Q}$. Соответственно, возникает вопрос, откуда брать эти группы. Известно, во всяком случае, что для $g \leqslant 7$ подходящие списки можно найти в статье [7].

Кроме того, даже в большей размерности можно заметно сузить список групп, подходящих на роль нужных нам групп Галуа. Для этого необходимо понимать, какие требования следует предъявить к этим группам. А именно, они должны удовлетворять следующим условиям:

а) G определяется с точностью до изоморфизма;

б) G является подгруппой симметрической группы S_{2g}, причем величина 2g должна делить порядок группы G;

в) G обладает нетривиальным центром, содержащим элемент порядка 2, который мы обозначим через ι;

г) G содержит подгруппу Δ порядка #G/2g, которая не является нормальной подгруппой в G и обладает тем свойством, что $\iota \notin \Delta$.

3. Классификация неразложимых BT_1-групповых схем. Конечная локально свободная коммутативная групповая схема G над схемой S называется усеченной групповой схемой Барсотти-Тейта уровня 1 или BT_1-групповой схемой, если она аннулируется отображением p и $\mathrm{Ker}(\mathrm{Frob}_G) = \mathrm{Im}(\mathrm{Ver}_G)$, где Frob_G — морфизм Фробениуса схемы G, Ver_G — двойственный к нему морфизм, а p — отображение «умножение на p».

В статье [21] приведена классификация неразложимых BT_1-групповых схем порядка p^{2g}, где $g \leqslant 3$. Это делается ровно для того, чтобы потом иметь возможность однозначно записать $A[p]$ как произведение конечного числа неразложимых BT_1-групповых схем. Однако как продолжить классификацию на произвольную размерность пока что остается открытым вопросом. Дело в том, что из статей [12; 14] известно, каким образом можно классифицировать произвольные конечные неразложимые групповые схемы, однако не всякая групповая схема, неразложимая в смысле Барсотти-Тейта, является неразложимой в обычном смысле, то есть не является представимой в виде произведения двух или более групповых схем (которые не обязательно сами будут являться BT_1-групповыми схемами). Возможно, для произвольной размерности потребуется ввести некий аналог теоремы из статьи [14], позволяющей классифицировать BT_1-групповые схемы через классификацию круговых слов определенного типа.

3. Постановка задачи

Принимая во внимание все вышесказанное, автору представляется возможным поставить перед собой следующие задачи:

1. Разработать способ классификации усеченных групповых схем Барсотти-Тейта уровня 1 в терминах круговых слов для любого наперед заданного порядка схемы.

2. Разработать и реализовать эффективный алгоритм, позволяющий за приемлемое время вычислять таблицу соответствий между разложениями идеала $p\mathcal{O}_K$ и разложениями групповой схемы $A[p]$ для не слишком больших размерностей абелева многообразия.

3. Разработать метод построения входных данных для алгоритма из пункта 2 для любых допускаемых им размерностей.

Список литературы

1. *Benger N., Charlemagne M., Freeman D. M.* On the Security of Pairing-Friendly Abelian Varieties over Non-prime Fields // Pairing-Based Cryptography–Pairing 2009, Lecture Notes in Comput. Sci., vol. 5671. Springer, 2009. P. 52—65.

2. *Blake C.* A Deuring criterion for abelian varieties // Bulletin of the London Mathematical Society. Dec. 2014. Vol. 46, issue 6. P. 1256.

3. *Bradford J.* Commutative Endomorphism Rings of Simple Abelian Varieties over Finite Fields. Ph.D. Thesis, University of Maryland, 2012.

4 *Clark P. L.* Bounds for torsion on abelian varieties with integral moduli // arXiv:math/0407264, 2004.

5. *Clark P. L., Xarles X.* Local bounds for torsion points on abelian varieties // Canad. J. Math. 2008. Vol. 60. P. 532—555.

6. *Demazure M.* Lectures on *p*-divisible groups // Lecture Notes in Mathematics, vol. 302. Berlin, 1986.

7. *Dodson B.* The structure of galois groups of cm-fields // ITransactions of the American Mathematical Society. 1984. № 283(1). P. 1—32.

8. *Ekedahl T.* On supersingular curves and abelian varieties // Math. Scand. 1987. № 60. P. 151—178.

9. *Van der Geer G.* Cycles on the moduli space of abelian varieties // Moduli of curves and abelian varieties, Aspects Math, E33. 1999. P. 65—89.

10. *Goren E.* On certain reduction problems concerning abelian surfaces // Manuscripta Math. 1997. № 94. P. 33—43.

11. *Goren E.* Lectures on Hilbert modular varieties and modular forms // CRM Monograph, vol. 14. AMS 2002.

12. *Kraft H.* Kommutative algebraische *p*-gruppen (mit anwendungen auf *p*-divisible gruppen und abelsche varietäten) // Manuscript, University of Bonn, September, 1985.

13. *Moonen B.* Group schemes with additional structures and Weyl group cosets // Moduli of Abelian varieties. 2001. Vol. 195. P. 255—298.

14. *Oort F.* Simple *p*-kernels of *p*-divisible groups // Advances in Mathematics. 2005. № 198. P. 275—310.

15. *Oort F.* A stratification of a moduli space of abelian varieties // Moduli of abelian varieties. 2001. Vol. 195. P. 345—416.

16. *Pries R.* A short guide to p-torsion of abelian varieties in characteristic *p* // arXiv:math/0609658v1, September, 2006.

17. *Ribet K.* Torsion points of abelian varieties in cyclotomic extensions // L'enseignement Mathématique. 1981. Vol. 27. P. 315—319.

18. *Sugiyama K.-I.* On a generalization of Deuring's results // Finite Fields and Their Applications. March 2014. Vol. 26. P. 69—85.

19. *Xarles X.* Torsion points of abelian varieties over p-adic fields // preprint. URL: http://mat.uab.es/~xarles/papers.htm.

20. *Yu C.-F.* A note on supersingular abelian varieties // arXiv:1412.7107, 2015.

21. *Zaytsev A.* Generalization of Deuring reduction theorem // Journal of Algebra. 2013. Vol. 392. P. 97—114.

Об авторе

Артём Смирнов — асп., Балтийский федеральный университет им. И. Канта, Калининград.

E-mail: AASmirnov@stud.kantiana.ru

About author

Artyom Smirnov — PhD student, I. Kant Baltic Federal University, Kaliningrad.

E-mail: AASmirnov@stud.kantiana.ru