Записки научных
семинаров ПОМИ
Том 523, 2023 г.

А. Л. Смирнов

О ГАУССОВЫХ КОЛЬЦАХ И АРГУМЕНТЕ ДЁЙРИНГА

§1. Введение

Понятие гауссового кольца введено в [1] и там же были приведены частичные результаты по классификации одномерных гауссовых колец. Цель этой заметки состоит в том, чтобы предъявить полную классификацию гауссовых колец размерности один. Еще одна цель – исправить некоторые неточности из [1].

Я благодарю О. Лоршида и других участников семинара по алгебраической геометрии над полем из одного элемента. Их замечания позволили понять, что классификация по существу содержится в уже опубликованных работах. Кроме того, я благодарю М. Концевича. Его замечание на одном из докладов автора позволило обнаружить исправляемую ниже неточность.

1.1. Напоминание. Напомним пару определений, необходимых для формулировки основного результата.

Определение 1.1.1. *Коммутативное кольцо A конечного типа над $\mathbb{Z}$ называется гауссовым, если*

(1) *A факториально;*
(2) *группа обратимых элементов A^* конечна.*

Определение 1.1.2. *Коммутативное кольцо A называется несократимым, если не существует изоморфизма вида $B[t] \simeq A$, где B некоторое кольцо.*

§2. Основные результаты

Легко видеть, что нульмерные гауссовы кольца это в точности конечные поля.

Ключевые слова: обобщенное кольцо, подход Дурова, поле из одного элемента, некоммутативный тензорный квадрат, одноклассное поле, гипотеза Римана.

2.1. Одномерные гауссовы кольца.

Теорема 2.1.1. *Пусть A — несократимое гауссово кольцо, причем $\dim A = 1$. Тогда A изоморфно одному из следующих колец: $\mathbb{Z}$, $\mathcal{O}_K$, $\Gamma(U, \mathcal{O}_U)$. При этом $K = \mathbb{Q}(\sqrt{-d})$, где $d = 3, 4, 7, 8, 11, 19, 43, 67, 163$, а U — гладкая аффинная алгебраическая кривая над полем F, где для пары (F, U) имеются следующие возможности.*

(1) $F = \mathbb{F}_2$, *U задано в* $\mathbf{A}^2$ *уравнением* $y^2 + y = x^3 + x + 1$.
(2) $F = \mathbb{F}_3$, *U задано в* $\mathbf{A}^2$ *уравнением* $y^2 = x^3 - x - 1$.
(3) $F = \mathbb{F}_4$, *U задано в* $\mathbf{A}^2$ *уравнением* $y^2 + y = x^3 + \eta$, $\eta^2 = \eta + 1$.
(4) $F = \mathbb{F}_2$, *U задано в* $\mathbf{A}^2$ *уравнением* $y^2 + y = x^5 + x^3 + 1$. *Это кривая рода* 2.
(5) $F = \mathbb{F}_2$, *поле $F(U)$ задано соотношением*
$$y^2 + y = (x^3 + x^2 + 1)(x^3 + x + 1)^{-1}.$$
Это кривая рода 2.
(6) $F = \mathbb{F}_2$, *U задано в* $\mathbf{A}^2$ *уравнением*
$$y^4 + xy^3 + (x^2 + x)y^2 + (x^3 + 1)y + (x^4 + x + 1) = 0.$$
Это кривая рода 3.
(7) $F = \mathbb{F}_2$, *U задано в* $\mathbf{A}^2$ *уравнением*
$$y^4 + (x^3 + x + 1)y + (x^4 + x + 1) = 0.$$
Это кривая рода 3.
(8) $F = \mathbb{F}_2$, *поле $F(U)$ задано соотношением*
$$y^5 + y^3 + y^2(x^3 + x^2 + x) + y(x^7 + x^5 + x^4 + x^3 + x)/(x^4 + x + 1) = (x^{13} + x^{12} + x^8 + x^6 + x^2 + x + 1)/(x^4 + x + 1).$$
Это кривая рода 4.

Доказательство. Теорема о классификации очень трудна, но в ее доказательстве нет заслуги автора данной заметки. Для доказательства достаточно собрать вместе известные результаты. Приведем необходимые ссылки и пояснения. По поводу классификации гауссовых одномерных колец нулевой характеристики см. [3] и [4]. Вторая часть этой теоремы, то есть часть, связанная с конечной характеристикой, доказана в работах [5–10]. □

Определение 2.1.2. *Будем говорить, что кольцо A мультипликативно неотличимо от $\mathbb{Z}$, если существует изоморфизм моноидов*

$\mathbb{Z}^\times \to A^\times$. *При этом для кольца* R *моноид* $R^\times$ *представляет собой* R *с забытым сложением.*

Следствие 2.1.3. *С точностью до изоморфизма имеется ровно десять дедекиндовых колец, мультипликативно неотличимых от* $\mathbb{Z}$. *А именно, кольцо* $\mathbb{Z}$, *кольца* $\mathbb{Z}[\omega]$, *где* $\omega = (1+\sqrt{-7})/2$, $\sqrt{-2}$, $(1+\sqrt{-11})/2$, $(1+\sqrt{-19})/2$, $(1+\sqrt{-43})/2$, $(1+\sqrt{-67})/2$, $(1+\sqrt{-163})/2$, *а также кольца* $\mathbb{F}_3[t]$ *и* $\mathbb{F}_3[x,y]/(y^2-x^3+x+1)$.

§3. Несколько замечаний

Начнем с некоторых исправлений и уточнений к [1].

3.1. Модули над некоторыми обобщенными кольцами. Мы будем иметь дело с обобщенными кольцами в смысле [2]. Равенство $\mathbb{Z}\otimes_{\mathbf{F}_1}\mathbb{Z} = \mathbb{Z}$ ставит под сомнение эвристическую основу подхода к гипотезе Римана с помощью обобщенных колец. Поэтому в [1] предпринята попытка использовать вместо обычного тензорного произведения его некоммутативную версию

$$S = \mathbb{Z} \boxtimes_{\mathbf{F}_1} \mathbb{Z}.$$

S-модуль представляет собой множество M с двумя структурами абелевой группы — обозначим соответствующие структурные данные нижними индексами 1 и 2. Например, пусть $x, y \in M$. Тогда их сумму, заданную первой структурой, обозначаем $x +_1 y$, а сумму, заданную второй структурой, обозначаем $x +_2 y$. Единственная связь между двумя структурами состоит в том, что $0_1 = 0_2$. Конечно, $S \neq \mathbb{Z}$, но категория S-Mod выглядит, на первый взгляд, как бесплодная математическая пустыня.

В этой пустыне, однако, имеется оазис. А именно, рассмотрим обобщенное кольцо

$$R = \mathbb{Z} \boxtimes_u \mathbb{Z}.$$

Здесь символ u взят из слова унарный. По определению R представляет собой фактор-кольцо некоммутативного тензорного произведения $\mathbb{Z} \boxtimes_{\mathbf{F}_1} \mathbb{Z}$ по соотношениям двух видов:

(1) коммутирование каждой унарной операции из первой копии $\mathbb{Z}$ и каждой операции (произвольной арности) из второй копии $\mathbb{Z}$;
(2) коммутирование каждой операции (произвольной арности) из первой копии $\mathbb{Z}$ и каждой унарной операции из второй копии $\mathbb{Z}$.

Заметим, что в геометрическом случае аналогичная конструкция приводит к обычному коммутативному тензорному произведению

$$\mathbb{F}_q[x] \boxtimes_u \mathbb{F}_q[x] = \mathbb{F}_q[x] \otimes_{\mathbb{F}_q} \mathbb{F}_q[x].$$

Действительно, дополнительные соотношения в этом случае означают перестановочность всех операций из двух структур, поскольку коммутативность операций старших арностей заложена в определения. Таким образом, произведение $\boxtimes_u$ можно назвать квазикоммутативным.

3.2. Модули над $\mathbb{Z} \boxtimes_u \mathbb{Z}$. Приведем явное описание R-модулей. Это, прежде всего, S-модуль, то есть множество M с двумя структурами абелевой группы, причем $0_1 = 0_2$. Кроме того (см. 3.1), должны быть выполнены следующие соотношения: $[m]_1[n]_2(x) = [n]_2[m]_1(x)$,

$$[m]_2(x +_1 y) = [m]_2(x) +_1 [m]_2(y), \quad [n]_1(x +_2 y) = [n]_1(x) +_2 [n]_1(y).$$

В частности, для выполнения дополнительных соотношений достаточно, чтобы были выполнены соотношения $[m]_1 = [m]_2$ ($m = \pm 1, \pm 2, \dots$).

3.3. Пример. Пара колец A_1 и A_2, мультипликативно неотличимых от $\mathbb{Z}$ (см. 2.1.2), дает семейство R-модулей $M(\sigma_1, \sigma_2)$, индексированное парой изоморфизмов моноидов

$$\sigma_i : \mathbb{Z}^\times \to A_i^\times.$$

Если такая пара σ_1, σ_2 выбрана, то соответствующий R-модуль строится следующим образом: $M(\sigma_1, \sigma_2) = \mathbb{Z}$, $[m]_i(x) = mx$, $x +_i y = \sigma_i^{-1}(\sigma_i(x) + \sigma_i(y))$.

3.4. Свойство Дёйринга. Положительный дискриминант Δ называют гауссовым, если множество классов бинарных квадратичных форм дискриминанта Δ состоит из одного класса. Для описания свойства Дёйринга удобно разбить последовательность положительных гауссовых дискриминантов на две части: спорадическую и серийную. К серийной части относятся те дискиминанты Δ, для которых $\Delta = 3 \bmod 8$. Таким образом, серийная часть представляет собой последовательность

$$3,\ 11,\ 19,\ 43,\ 67,\ 163, \dots \tag{1}$$

Легко проверяется (см. [4]), что множество спорадических гауссовых дискриминантов совпадает с множеством $\{4, 7, 8\}$, а каждый серийный

дискриминант – простое число. В данный момент мы знаем, что других чисел в последовательности (1) нет. Однако до работы [11] даже конечность этой последовательности была под вопросом.

Теорема 3.4.1 (свойство Дёйринга)**.** *Если имеется бесконечно много гауссовых дискриминантов* Δ*, то*

$$\zeta(s)\lim_{\Delta} L(\Delta, s) = \zeta(2s),$$

где $L(\Delta, s)$ *означает L-ряд, соответствующий квадратичному расширению* $\mathbb{Q}(\sqrt{-\Delta})$.

Эта теорема доказана в [11, Satz 3]. Ее значение обсуждается ниже в 3.6. Доказательство теоремы 3.4.1, хотя и коротко, но опирается на ряд оценок. Попробуем прояснить его смысл.

3.5. Эвристическое объяснение свойства Дёйринга. Пусть Δ серийный гауссов дискриминант. Тогда кольцо целых поля $\mathbb{Q}(\sqrt{-\Delta})$ имеет вид $\mathbb{Z}[\omega]$, где ω корень полинома

$$f = x^2 - x + (\Delta + 1)/4.$$

При $\Delta = 43$, например, получим $f = x^2 - x + 11$. Рассмотрим следующее утверждение:

$$f \bmod p \text{ неприводим для всех простых } p < (\Delta + 1)/4. \tag{2}$$

При $\Delta = 43$ речь идет о неприводимости полиномов $x^2 - x + 11 \bmod 2$, $x^2 - x + 11 \bmod 3$, $x^2 - x + 11 \bmod 5$, $x^2 - x + 11 \bmod 7$.

Предположим, что утверждение (2) верно. Пусть $\zeta(\Delta, s)$ означает ζ-функцию Дедекинда поля $\mathbb{Q}(\sqrt{-\Delta})$. По определению,

$$\zeta(\Delta, s) = \prod_{\pi} \frac{1}{1 - \mathrm{Norm}(\pi)^{-s}}, \tag{3}$$

где π пробегает множество P, состоящее из простых ненулевых идеалов кольца целых в $\mathbb{Q}(\sqrt{-\Delta})$. Выделим в P подмножество

$$S = \{\pi \in P \mid \text{положительный генератор идеала } \pi \cap \mathbb{Z} \text{ меньше } (\Delta+1)/4\}.$$

Соответственно, разобьем произведение (3) на две части

$$\zeta(\Delta, s) = \prod_{\pi \in S} \frac{1}{1 - \mathrm{Norm}(\pi)^{-s}} \prod_{\pi \notin S} \frac{1}{1 - \mathrm{Norm}(\pi)^{-s}}. \tag{4}$$

Утверждение (2) означает, что первый из двух множителей в (4) имеет вид

$$\prod_{p<(\Delta+1)/4} \frac{1}{1-p^{-2s}}.$$

Таким образом, начало эйлерова произведения для $\zeta(\Delta, s)$ такое же, как и для $\zeta(2s)$. Поэтому для достаточно больших Δ имеется приближенное равенство

$$\zeta(\Delta, s) \approx \zeta(2s).$$

Если бы существовало сколь угодно большое Δ, то есть гауссовых дискриминантов было бы бесконечно много, то было бы естественно предположить, что

$$\lim_{\Delta} \zeta(\Delta, s) = \zeta(2s). \tag{5}$$

Так как $\zeta(\Delta, s) = \zeta(s)L(\Delta, s)$, то ввиду (5) можно было бы предположить, что $\zeta(s) \lim_{\Delta} L(\Delta, s) = \zeta(2s)$. Именно это и доказал Дёйринг.

3.6. Связи с гипотезой Римана. Конечность последовательности гауссовых дискриминантов (1) доказана в [11], причем весьма удивительным способом. Прежде всего, Гекке доказал (см. [12]), что гипотеза Римана влечет конечность (1). Это не удивляет, так как из гипотезы Римана вытекает немало интересного. Удивительно то, что гипотеза Римана выведена из бесконечности последовательности (1). Основную роль при этом играет свойство Дёйринга (3.4.1), от которого до гипотезы Римана рукой подать. Таким образом, из бесконечности (1) вытекает гипотеза Римана, а из нее конечность (1). Поэтому последовательность (1) конечна, независимо от верности гипотезы Римана.

Казалось бы, конечность последовательности гауссовых дискриминантов и тем более полнота списка Гаусса, делают рассуждение Дёйринга полносью ненужным. Это действительно так, если отнестись к этому рассуждению чисто формально. Однако неожиданно кольца, связанные со списком Гаусса, пригодились при построении интересных модулей над обобщенным кольцом $\mathbb{Z} \boxtimes_u \mathbb{Z}$. Для применения этого кольца к гипотезе Римана необходимы, по меньшей мере, два обстоятельства.

Во-первых, категория модулей $\mathbb{Z}\boxtimes_u\mathbb{Z}$-Mod должна быть достаточно сложной и интересной. Во-вторых, должно быть что-то вроде подхода к гипотезе Римана, использующее это кольцо. Рассуждение Дёйринга интересно тем, что имеет непосредственное отношение к обоим обстоятельствам.

Список литературы

1. А. Л. Смирнов, *О сложениях на мультипликативном моноиде целых чисел.* — Зап. научн. семин. ПОМИ, **502** (2021), 139–151.
2. N. Durov, *New Approach to Arakelov Geometry.* — `arXiv: 0704.2030 v1 [math AG] 16 Apr 2007`.
3. D. Goldfeld, *Gauss' class number problem for imaginary quadratic fields.* — Bull. of AMS **13**, Number 1, July 1985.
4. И. Р. Шафаревич, *Проблема десятого дискриминанта.* — Алгебра и анализ **25**, No. 4 (2013), 260–277.
5. R. E. MacRae, *On Unique Factorization in Certain Rings of Algebraic Functions.* — J. of Algebra **17** (1971), 243–261.
6. M. L. Madan, C. S. Queen, *Algebraic Function Fields of class number one.* — Acta Arithmetica XX, 424–431 (1972).
7. J. R. C. Leitzel, M. L. Madan, C. S. Queen, *Algebraic Function Fields with Small Class Number.* — J. Number Theory **7** (1975), 11–27.
8. C. Stirpe, *A counterexample to 'Algebraic function fields with small class number'.* — J. Number Theory, **143** (2014), 402–404.
9. P. Mercuri, C. Stirpe, *Classification of algebraic function fields with class number one.* — `arXiv: 1406.5365v3, 2014.`
10. Q. Shen, S. Shi, *Function fields of class number one.* — NY Number Theory Conference, 2015.
11. M. Deuring, *Imaginare quadratische Zahlkörper mit der Klassenzahl 1.* — Math. Z. **37** (1933), 405–415.
12. E. Landau, *Über die Klassenzahl imaginär-quadratische Zahlkörper.* — Gött. Nachr. (1918), 285–295.

Smirnov A. L. On Gauss' rings and Deuring's argument.

The Dedekind rings multiplicativly indistinguishable with $\mathbb{Z}$ are classified. Certain inaccuracies of a previous paper are corrected. Deuring's reasoning related to the Riemann conjecture and the finiteness of the list of Gauss' class number problem for imaginary quadratic 10-th discriminant problem are heuvristically explained.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова
E-mail: `smirnov@pdmi.ras.ru`

Поступило 23 октября 2023 г.