

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.17

DOI 10.17223/20710410/56/1

ИССЛЕДОВАНИЕ ГРУППЫ АВТОМОРФИЗМОВ КОДА, АССОЦИИРОВАННОГО С ОПТИМАЛЬНОЙ КРИВОЙ РОДА ТРИ¹

Е. С. Малыгина

*Балтийский федеральный университет им. И. Канта, г. Калининград, Россия***E-mail:** emalygina@kantiana.ru

Доказано, что отображение обладает свойством мультипликативности на соответствующем пространстве Римана — Роха, ассоциированного с дивизором mP_∞ , который определяет некоторый алгебро-геометрический код (АГ-код), если число точек степени один функционального поля оптимальной кривой рода три, определённой над конечным полем с дискриминантом из $\{-19, -43, -67, -163\}$, имеет нижнюю границу $12m/(m-3)$. С помощью явного вычисления нормирования дивизоров полюсов образов базисных функций x, y, z функционального поля кривой при отображении λ установлено, что группа автоморфизмов функционального поля кривой является подгруппой автоморфизмов соответствующего АГ-кода. Доказано также, что при $m \geq 4$ и $n > 12m/(m-3)$ группа автоморфизмов функционального поля кривой изоморфна группе автоморфизмов АГ-кода, который ассоциирован с дивизорами $\sum_{i=1}^n P_i$ и mP_∞ , где P_i — точки степени один рассматриваемого функционального поля.

Ключевые слова: оптимальная кривая, алгебро-геометрический код, функциональное поле, группа автоморфизмов кода.

INVESTIGATION OF AUTOMORPHISM GROUP FOR CODE ASSOCIATED WITH OPTIMAL CURVE OF GENUS THREE

E. S. Malygina

Immanuel Kant Baltic Federal University, Kaliningrad, Russia

The main result of this paper is contained in two theorems. In the first theorem, it is proved that the mapping $\lambda : \mathcal{L}(mP_\infty) \rightarrow \mathcal{L}(mP_\infty)$ has the multiplicative property on the corresponding Riemann — Roch space associated with the divisor mP_∞ which defines some algebraic-geometric code if the number of points of degree one in the function field of genus three optimal curve over finite field with a discriminant $\{-19, -43, -67, -163\}$ has the lower bound $12m/(m-3)$. Using an explicit calculation with the valuations of the pole divisors of the images of the basis functions x, y, z in the function field of the curve via the mapping λ , we have proved that the automorphism

¹Работа выполнена при финансовой поддержке Программы мобильности 5-100, а также при финансовой поддержке Минобрнауки России (соглашение № 075-02-2022-872).

group of the function field of our curve is a subgroup in the automorphism group of the corresponding algebraic-geometric code. In the second theorem, it is proved that if $m \geq 4$ and $n > 12m/(m-3)$, then the automorphism group of the function field of our curve is isomorphic to the automorphism group of the algebraic-geometric code associated with divisors $\sum_{i=1}^n P_i$ and mP_∞ , where P_i are points of the degree one.

Keywords: *optimal curve, algebraic-geometric code, function field, automorphism group of AG-code.*

Введение

Алгебро-геометрические коды (АГ-коды), также известные как коды Гошпы, впервые были представлены в [1]. В действительности, можно ассоциировать коды с дивизорами функциональных полей, тем самым рассматривая теорию кодирования с точки зрения алгебраической геометрии. Многие известные на сегодняшний день коды являются АГ-кодами или подмножествами АГ-кодов, что позволяет изучать их с алгебро-геометрической точки зрения. В этой работе мы рассмотрим приложения алгебраической геометрии исключительно с алгебраической точки зрения. Преимущество такого подхода позволяет взять за основу лишь некоторые базовые знания, касающиеся алгебраических расширений полей.

Улучшение границы Варшавова — Гилберта оказалось существенным прорывом в теории кодирования и позволило с большим интересом взглянуть на кривые с большим числом точек, а именно на их приложения. Знание группы автоморфизмов АГ-кода или даже её части примечательно тем, что позволяет получить информацию о структуре самого кода и зачастую может быть использовано в алгоритме декодирования.

В своё время Х. Штихтенот представил доказательство того, что при определённых условиях группа автоморфизмов рационального АГ-кода изоморфна некоторой подгруппе автоморфизмов соответствующего поля рациональных функций [2]. Чуть позже этот подход был обобщён Ч. Ксингом для специального класса эллиптических кодов [3] и эрмитовых кодов [4]. Вопрос подобного исследования для негиперэллиптических кривых рода ≥ 3 на сегодняшний день остаётся открытым.

Данная работа посвящена исследованию группы автоморфизмов АГ-кодов, построенных на оптимальных кривых рода три, не являющихся гиперэллиптическими. Её суть заключается в установлении условия, связывающего число точек одного дивизора и кратность бесконечной точки второго дивизора. Оба этих дивизора ассоциированы с АГ-кодом, группа автоморфизмов которого изоморфна группе автоморфизмов соответствующего функционального поля оптимальной кривой.

В работе в качестве предварительных сведений представлены основная теоретическая база, касающаяся функциональных полей, и определение и свойства оптимальной кривой рода три. Ядром работы являются две теоремы: в первой определено условие, позволяющее сузить автоморфизмы функционального поля на пространство Римана — Роха, а далее рассмотреть их как автоморфизмы соответствующего АГ-кода; во второй теореме доказано наличие изоморфизма между группой автоморфизмов АГ-кода и группой автоморфизмов функционального поля кривой.

Предварительные результаты данной работы были представлены на конференции SIBECRYPT'18 [5].

1. Предварительные сведения

1.1. Общая теория функциональных полей

На протяжении всех предварительных сведений под K будем понимать произвольное поле, при необходимости внося уточнения.

Определение 1. Алгебраическим функциональным полем F/K от одной переменной называется расширение F поля K , такое, что F является конечным алгебраическим расширением $K(x)$ для некоторого элемента $x \in F$, являющегося трансцендентным над K .

Для краткости будем называть F/K просто функциональным полем. Будем считать известным понятие кольца нормирования функционального поля [6, Definition 1.1.4]. Здесь лишь упомянем о кольце нормирования точки P , подразумевая под P максимальный идеал кольца нормирования поля F/P :

$$\mathcal{O}_P = \{z \in F : z^{-1} \notin P\}.$$

При этом множество всех точек функционального поля F/K будем обозначать $\mathbb{P}_F$. Определим степень точки P функционального поля F/K как $\deg P = [\mathcal{O}_P/P : K]$.

Напомним, что, согласно [6], всякий элемент $0 \neq z \in F$ имеет единственное представление $z = t^n u$, если $P = t\mathcal{O}_P$, $u \in \mathcal{O}_P^*$ и $n \in \mathbb{Z}$.

Определение 2. С каждой точкой $P \in \mathbb{P}_F$ ассоциируем функцию

$$v_P : F \rightarrow \mathbb{Z} \cup \{\infty\},$$

которая играет роль дискретного нормирования функционального поля F/K :

$$v_P(z) = n \text{ для } z = t^n u, \quad v_P(0) = \infty.$$

Будем говорить, что точка P имеет нуль в z тогда и только тогда, когда $v_P(z) > 0$, и имеет полюс в z тогда и только тогда, когда $v_P(z) < 0$.

Отметим также, что дискретное нормирование v_P поля F/K удовлетворяет строгому неравенству треугольника

$$v_P(x + y) = \min\{v_P(x), v_P(y)\}, \quad (1)$$

если $v_P(x) \neq v_P(y)$ для $x, y \in F$.

Определение 3. Абелева группа $\mathcal{D}_F$, порождённая точками функционального поля F/K , называется группой дивизоров поля F/K .

Элементы группы $\mathcal{D}_F$ называются дивизорами поля F/K . Дивизор представляет собой формальную сумму точек:

$$D = \sum_{P \in \mathbb{P}_F} n_P P, \text{ где } n_P \in \mathbb{Z} \text{ и почти все } n_P = 0.$$

Носителем дивизора D является множество

$$\text{supp}(D) = \{P \in \mathbb{P}_F : n_P \neq 0\}.$$

Для $P \in \mathbb{P}_F$ и дивизора D определим $v_P(D) = n_P$. Таким образом,

$$D = \sum_{P \in \text{supp}(D)} v_P(D) P.$$

На $\mathcal{D}_F$ определено также частичное упорядочивание, а именно:

$$D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2) \text{ для всех } P \in \mathbb{P}_F.$$

Степень дивизора определяется гомоморфизмом $\deg : \mathcal{D}_F \rightarrow \mathbb{Z}$:

$$\deg D = \sum_{P \in \mathbb{P}_F} v_P(D) \deg P.$$

Определение 4. Пусть $x \in F^*$. Обозначим через Z (через N) множество нулей (полюсов) x в $\mathbb{P}_F$. Тогда для функции x определим её дивизор нулей:

$$(x)_0 = \sum_{P \in Z} v_P(x) P;$$

дивизор полюсов:

$$(x)_\infty = \sum_{P \in N} (-v_P(x)) P;$$

главный дивизор:

$$(x) = (x)_0 - (x)_\infty.$$

Дадим определение пространству Римана — Роха, одному из главных понятий в теории функциональных полей.

Определение 5. Для дивизора $D \in \mathcal{D}_F$ положим

$$\mathcal{L}(D) = \{x \in F : (x) \geq -D\} \cup \{0\}.$$

Данное множество называется пространством Римана — Роха, ассоциированным с дивизором D . Отметим, что $\mathcal{L}(D)$ является конечномерным векторным пространством над полем K . Целое $\dim D = \dim \mathcal{L}(D)$ называется размерностью дивизора D .

Определение 6. Род функционального поля F/K определён следующим образом:

$$g = \max\{\deg D - \dim D + 1 : D \in \mathcal{D}_F\}.$$

1.2. Алгебро-геометрические коды

Покажем, как задаётся код, ассоциированный с функциональным полем. Такие коды, как уже было сказано, называются геометрическими кодами Гошпы или АГ-кодами. Зафиксируем следующие обозначения:

- $F/\mathbb{F}_p$ — алгебраическое функциональное поле рода g ;
- $P_1, P_2, \dots, P_n$ — попарно различные точки поля $F/\mathbb{F}_p$ степени один;
- $D = P_1 + \dots + P_n$;
- G — дивизор поля $F/\mathbb{F}_p$, такой, что $\text{supp}(G) \cap \text{supp}(D) = \emptyset$.

Определение 7. АГ-код $\mathcal{C}_{\mathcal{L}}(D, G)$, ассоциированный с дивизорами D и G , определён следующим образом:

$$\mathcal{C}_{\mathcal{L}}(D, G) = \{(x(P_1), \dots, x(P_n)) : x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_p^n.$$

Рассмотрим отображение

$$ev_D : \begin{cases} \mathcal{L}(G) \rightarrow \mathbb{F}_p^n, \\ ev_D(x) = (x(P_1), \dots, x(P_n)) \in \mathbb{F}_p^n. \end{cases}$$

Это отображение $\mathbb{F}_p$ -линейно, а код $\mathcal{C}_{\mathcal{L}}(D, G)$ является образом пространства Римана — Роха $\mathcal{L}(G)$ относительно этого отображения. Если, кроме того, $\deg G < n$, то ev_D — биекция на $\mathcal{C}_{\mathcal{L}}(D, G)$.

Отметим, что, согласно [6, Theorem 2.2.2], $\mathcal{C}_{\mathcal{L}}(D, G)$ является $[n, k, d]$ -кодом с параметрами $k = \dim G - \dim(G - D)$ и $d \geq n - \deg G$.

Прежде чем рассмотреть автоморфизмы АГ-кодов, рассмотрим автоморфизмы соответствующего функционального поля $F/\mathbb{F}_p$, которые образуют группу относительно композиции функций:

$$\text{Aut}(F/\mathbb{F}_p) = \{\sigma : \sigma(a) = a, a \in \mathbb{F}_p\}.$$

Группа $\text{Aut}(F/\mathbb{F}_p)$ действует на точки $\mathbb{P}_F$ как $\sigma(P) = \{\sigma(x) : x \in P\}$, при этом $\deg \sigma(P) = \deg P$. Действие $\text{Aut}(F/\mathbb{F}_p)$ на $\mathbb{P}_F$ можно продолжить до действия на группу дивизоров, полагая

$$\sigma(\sum n_P P) = \sum n_P \sigma(P).$$

Под группой автоморфизмов произвольного кода $\mathcal{C} \subseteq \mathbb{F}_p^n$ будем понимать

$$\text{Aut}(\mathcal{C}) = \{\pi \in S_n : \pi(\mathcal{C}) = \mathcal{C}\},$$

где S_n — симметрическая группа.

Определение 8. Определим

$$\text{Aut}_{D,G}(F/\mathbb{F}_p) = \{\sigma \in \text{Aut}(F/\mathbb{F}_p) : \sigma(D) = D, \sigma(G) = G\}.$$

Отметим, что автоморфизм $\sigma \in \text{Aut}_{D,G}(F/\mathbb{F}_p)$ не обязательно фиксирует все точки $P_1, \dots, P_n$, однако действует на них как перестановка. Окончательно получаем, что

$$\sigma(\mathcal{L}(G)) = \mathcal{L}(G),$$

поскольку $\sigma \in \text{Aut}(F/\mathbb{F}_p)$ и $\sigma(G) = G$. Следующий результат показывает, что каждый автоморфизм $\sigma \in \text{Aut}(F/\mathbb{F}_p)$ индуцирует автоморфизм соответствующего кода $\mathcal{C}_{\mathcal{L}}(D, G)$.

Теорема 1 [6, Proposition 8.2.3].

1) Действие группы $\text{Aut}_{D,G}(F/\mathbb{F}_p)$ на код $\mathcal{C}_{\mathcal{L}}(D, G)$ задано следующим образом:

$$\sigma((x(P_1), \dots, x(P_n))) = (x(\sigma(P_1)), \dots, x(\sigma(P_n)))$$

для $x \in \mathcal{L}(G)$ и $\sigma \in \text{Aut}_{D,G}(F/\mathbb{F}_p)$. Такое отображение является гомоморфизмом групп $\text{Aut}_{D,G}(F/\mathbb{F}_p) \rightarrow \text{Aut}(\mathcal{C}_{\mathcal{L}}(D, G))$.

2) Если $n > 2g + 2$, где g — род поля $F/\mathbb{F}_p$, то этот гомоморфизм инъективен и, следовательно, группу автоморфизмов $\text{Aut}_{D,G}(F/\mathbb{F}_p)$ можно рассматривать как подгруппу в $\text{Aut}(\mathcal{C}_{\mathcal{L}}(D, G))$.

Согласно теореме 1, если $\deg D > 2g + 2$, то $\text{Aut}_{D,G}(F/\mathbb{F}_p)$ может быть вложена в $\text{Aut}(\mathcal{C}_{\mathcal{L}}(D, G))$. Можно ассоциировать с каждым автоморфизмом π кода $\mathcal{C}_{\mathcal{L}}(D, G)$ линейный автоморфизм, обозначим его за λ_π , ассоциированного пространства Римана — Роха $\mathcal{L}(G)$. Автоморфизм λ_π является сужением на $\mathcal{L}(G)$ автоморфизма $\bar{\lambda} \in \text{Aut}(F/\mathbb{F}_p)$ в том смысле, что $\bar{\lambda}|_{\mathcal{L}(G)}$ — линейное отображение и совпадает с λ_π на $\mathcal{L}(G)$ как $\mathbb{F}_p$ -линейное отображение. Окончательно, $\bar{\lambda} \in \text{Aut}_{D,G}(F/\mathbb{F}_p)$ и индуцирует π с помощью вложения $\text{Aut}_{D,G}(F/\mathbb{F}_p) \hookrightarrow \text{Aut}(\mathcal{C}_{\mathcal{L}}(D, G))$. В русле сказанного справедливо следующее

Определение 9. Пусть заданы два дивизора $D = P_1 + \dots + P_n$ и $D' = P'_1 + \dots + P'_n$, где $P_i, P'_i \in \mathbb{P}_{\mathbb{F}}$ — точки степени один. Пусть G — дивизор, такой, что $\text{supp}(G) \cap \text{supp}(D) = \emptyset$ и $\text{supp}(G) \cap \text{supp}(D') = \emptyset$, $\deg G < n$. Если $\mathcal{C}_{\mathcal{L}}(D, G) = \mathcal{C}_{\mathcal{L}}(D', G)$, то определим $\mathbb{F}_p$ -линейное отображение $\lambda : \mathcal{L}(G) \rightarrow \mathcal{L}(G)$ следующим образом:

$$\begin{array}{ccc} \mathcal{C}_{\mathcal{L}}(D, G) & \xrightarrow{\text{id}} & \mathcal{C}_{\mathcal{L}}(D', G) \\ \uparrow \text{ev}_D & & \downarrow \text{ev}_{D'}^{-1} \\ \mathcal{L}(G) & \xrightarrow{\lambda = \text{ev}_{D'}^{-1} \circ \text{ev}_D} & \mathcal{L}(G) \end{array}$$

Отметим, что корректность определения опирается на тот факт, что отображения ev_D и $\text{ev}_{D'}$ являются $\mathbb{F}_p$ -биективными на $\mathcal{C}_{\mathcal{L}}(D, G)$.

Для всех $x \in \mathcal{L}(G)$ мы можем выразить $\lambda(x) \in \mathcal{L}(G)$ как $\lambda(x)(P'_i) = x(P_i)$ для $i = 1, \dots, n$.

1.3. Определение и свойства оптимальной кривой

Определение 10. Пусть C — гладкая неприводимая проективная кривая рода g , определённая над конечным полем $\mathbb{F}_p$. Будем называть кривую C оптимальной, если число её рациональных точек удовлетворяет границе Хассе — Вейля — Серра

$$\#C(\mathbb{F}_p) = p + 1 \pm g[2\sqrt{p}].$$

В случае «−» кривая будет минимальной, в случае «+» — максимальной.

Согласно [7, Theorem 5.1], оптимальную кривую рода три можно задать явно. В работе рассмотрим лишь кривые, заданные уравнениями

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \beta_0 y, \\ y^2 = x^3 + ax + b, \end{cases} \quad (2)$$

где $\alpha_0, \alpha_1, \alpha_2, \beta_0, a, b \in \mathbb{F}_p$.

Под дискриминантом конечного поля $\mathbb{F}_p$ будем понимать число

$$d(\mathbb{F}_p) = [2\sqrt{p}]^2 - 4p.$$

Замечание 1. Отметим, что, согласно [8], оптимальные кривые существуют также над конечными полями с дискриминантами $\{-43, -67, -163\}$ и могут быть заданы явно с помощью уравнения (2). Кроме того, такие кривые не являются гиперэллиптическими.

Теорема 2 [8, Предложение 3.1.5, с. 60]. Пусть C — оптимальная кривая рода три над конечным полем $\mathbb{F}_p$ с дискриминантом $d(\mathbb{F}_p) \in \{-19, -43, -67, -163\}$. Тогда

$$\text{Aut}_{\mathbb{F}_p}(C) \cong D_3,$$

где D_3 — группа диэдра порядка 6.

1.4. Функциональное поле, ассоциированное с оптимальной кривой рода три

Рассмотрим функциональное поле $F/\mathbb{F}_p$. Существует неособая проективная кривая C (с точностью до изоморфизма), чьё функциональное поле $\mathbb{F}_p(C)$ изоморфно над $\mathbb{F}_p$ полю F . Кривая C может быть построена следующим образом: выбираются

$x, y, z \in F$, такие, что $F = \mathbb{F}_p(x, y, z)$. Пусть $f(X, Y, Z) \in \mathbb{F}_p[X, Y, Z]$ — неприводимый многочлен, такой, что $f(x, y, z) = 0$. Положим $W = \{P \in \mathbb{A}^3 : f(P) = 0\}$ и $\bar{W} \subseteq \mathbb{P}^3$ — проективное замыкание множества W . Полагая, что C — несингулярная модель $\bar{W}$, получаем, что $\mathbb{F}_p(C) \cong F$. Поэтому впредь будем отождествлять понятие кривой и её функционального поля.

Следующий результат достаточно элементарен, однако он понадобится для доказательства одной из основных теорем.

Теорема 3. Пусть дана башня числовых полей $K \subset K(x, y) \subset F = K(x, y, z)$, где x, y трансцендентны над K и $f(x, y, Z)$ — минимальный многочлен элемента z над $K(x, y)$. Предположим, что $\tilde{x}, \tilde{y}, \tilde{z} \in F \setminus K$ и пусть $f(\tilde{x}, \tilde{y}, \tilde{z}) = 0$. Тогда отображение

$$\lambda : \begin{cases} F/K \rightarrow F/K, \\ g(x, y, z) \mapsto g(\tilde{x}, \tilde{y}, \tilde{z}) \end{cases}$$

является K -эндоморфизмом поля F . Кроме того, если $x, y, z \in \text{Im } \lambda$, то λ — автоморфизм расширения F/K .

Доказательство. Так как $\tilde{x}, \tilde{y}$ трансцендентны над K , то отображение

$$\lambda_1 : \begin{cases} K[x, y] \rightarrow K[\tilde{x}, \tilde{y}], \\ g(x, y) \mapsto g(\tilde{x}, \tilde{y}) \end{cases}$$

является изоморфизмом колец. Этот изоморфизм можно продолжить на поле дробей:

$$\lambda_1 \rightsquigarrow \lambda_2 : \begin{cases} K(x, y) \rightarrow K(\tilde{x}, \tilde{y}), \\ g(x, y) \mapsto g(\tilde{x}, \tilde{y}). \end{cases}$$

В этом случае λ_2 также является изоморфизмом и индуцирует изоморфизм колец:

$$\lambda_2 \rightsquigarrow \lambda_3 : \begin{cases} K(x, y)[Z] \rightarrow K(\tilde{x}, \tilde{y})[Z], \\ g(x, y, Z) \mapsto g(\tilde{x}, \tilde{y}, Z). \end{cases}$$

Окончательно получаем отображение λ_4 :

$$\underbrace{K(x, y)[Z] \xrightarrow{\lambda_3} K(\tilde{x}, \tilde{y})[Z] \xrightarrow{\sigma} K(\tilde{x}, \tilde{y})[\tilde{z}]}_{\lambda_4 = \sigma \circ \lambda_3},$$

являющееся гомоморфизмом колец, где σ вычисляет значение рациональной функции от $\tilde{x}, \tilde{y}$ и переменной Z в точке $\tilde{z}$, т.е. $\sigma(g(\tilde{x}, \tilde{y}, Z)) = g(\tilde{x}, \tilde{y}, \tilde{z})$. Поскольку $\text{Ker } \lambda_4 = (f(x, y, Z))$, то

$$F = K(x, y)[Z]/(f(x, y, Z)) \cong K(\tilde{x}, \tilde{y})[\tilde{z}] = K(\tilde{x}, \tilde{y})(\tilde{z}) \subseteq F.$$

Таким образом, отображение λ , индуцированное с помощью λ_4 , является желаемым K -эндоморфизмом поля F . ■

Замечание 2. Рассмотрим функциональное поле $F/\mathbb{F}_p$ нашей оптимальной кривой. Согласно рассуждениям, представленным в [7], отметим, что

- 1) F не является рациональным;
- 2) существует точка $P_\infty \in \mathbb{P}_F$, $\deg P_\infty = 2$, и элементы $x, y, z \in F$, такие, что дивизоры полюсов этих функций имеют вид $(x)_\infty = (z)_\infty = 2P_\infty$, $(y)_\infty = 3P_\infty$;
- 3) для $m \geq 0$ элементы $x^i y^j z^k$ образуют базис пространства $\mathcal{L}(mP_\infty)$, где $i \geq 0$, $0 \leq j, k \leq 1$ и $2i + 3j + 2k \leq m$.

2. Основной результат

Исследуем класс алгебраических функциональных полей, которые не являются ни эллиптическими, ни гиперэллиптическими. Этот класс функциональных полей ассоциирован с оптимальными кривыми рода три. Покажем, при каких условиях группа автоморфизмов функционального поля совпадает с группой автоморфизмов соответствующего АГ-кода.

Зафиксируем некоторые обозначения:

- F — функциональное поле оптимальной кривой C ;
- $J \subseteq \mathbb{P}_F \setminus \{P_\infty\}$;
- $n = |J|$;
- $D = \sum_{P \in J} P = P_1 + P_2 + \dots + P_n$;
- $D' = \sum_{r=1}^n P_{\pi(r)}$ для некоторой перестановки $\pi \in S_n$.

В представленной далее теореме мы неоднократно будем ссылаться на следующий результат:

Лемма 1. Пусть $u, v \in \mathcal{L}(G)$ для некоторого дивизора $G = G_0 - G_1$, где $G_0, G_1 \geq 0$; $r = \deg G_0$; $P_1, P_2, \dots, P_n$ — различные точки степени один, не лежащие в носителе дивизора G_0 . Если $u(P_i) = v(P_i)$ для $i = 1, \dots, n$ и $n > r$, то $u = v$.

Доказательство. Поскольку $\mathcal{L}(G)$ — векторное пространство, то $u - v \in \mathcal{L}(G)$. Следовательно, $\deg((u - v)_\infty) \leq r$. Однако функция $u - v$ имеет, как минимум, $n > r$ нулей, так как $(u - v)(P_i) = 0$ и $v_{P_i}(u - v) \geq 1$ для $i = 1, \dots, n$. Принимая во внимание факт, что $\deg((u - v)_0) = \deg((u - v)_\infty)$ [6, Theorem 1.4.11], единственным вариантом является $u - v = 0$. ■

Нам потребуется установить взаимосвязь числа точек дивизора D с параметром m , где $G = mP_\infty$.

Теорема 4. Пусть $m \geq 4$ и $x, y, z \in \mathcal{L}(mP_\infty)$. Предположим, что $\mathcal{C}_{\mathcal{L}}(D, mP_\infty) = \mathcal{C}_{\mathcal{L}}(D', mP_\infty)$. Определим отображение $\lambda : \mathcal{L}(mP_\infty) \rightarrow \mathcal{L}(mP_\infty)$ так же, как в определении 9. Если выполняются следующие условия:

- 1) $-v_{P_\infty}(\lambda(x)) \leq c$, где $c \leq m$;
- 2) $n > 12m/(m - 3)$,

то $v_{P_\infty}(\lambda(x)) = v_{P_\infty}(\lambda(z)) = -2$ и $v_{P_\infty}(\lambda(y)) = -3$. Кроме того, λ является сужением автоморфизма функционального поля кривой на $\mathcal{L}(mP_\infty)$.

Доказательство. Для $0 \leq j, k \leq 1$ определим $\alpha_{ij} = \lfloor (m - 3j - 2k)/2 \rfloor$. Тогда, очевидно, имеем

$$\begin{aligned} \mathcal{L}(mP_\infty) = \langle & 1, x, x^2, \dots, x^{\alpha_{00}}; \\ & y, xy, x^2y, \dots, x^{\alpha_{10}}y; \\ & z, xz, x^2z, \dots, x^{\alpha_{01}}z; \\ & yz, xyz, x^2yz, \dots, x^{\alpha_{11}}yz \rangle. \end{aligned}$$

Докажем, что λ действует мультипликативно на $\mathcal{L}(mP_\infty)$. Другими словами, если $x^i y^j z^k \in \mathcal{L}(mP_\infty)$, то $\lambda(x^i y^j z^k) = \lambda(x)^i \lambda(y)^j \lambda(z)^k$ для $i \geq 0$, $0 \leq j, k \leq 1$. В ходе доказательства этого факта мы определим оценки степеней дивизоров полюсов функций $\lambda(x)$, $\lambda(y)$ и $\lambda(z)$.

Из условия теоремы 4 и того, что $(x)_\infty = (z)_\infty = 2P_\infty$, $(y)_\infty = 3P_\infty$, имеем

$$\begin{aligned} 4 &\leq \deg((\lambda(x)_\infty)) \leq c; \\ 4 &\leq \deg((\lambda(y)_\infty)), \deg((\lambda(z)_\infty)) \leq m. \end{aligned}$$

Покажем, что $\lambda(x)$, $\lambda(y)$ и $\lambda(z)$ удовлетворяют уравнению (2) функционального поля кривой и, следовательно, определяют эндоморфизм $\tilde{\lambda}$ поля $F/\mathbb{F}_q$, такой, что $\tilde{\lambda} = \lambda|_{\mathcal{L}(mP_\infty)}$. Поскольку $x, y, z \in \text{Im } \lambda$, то $x, y, z \in \text{Im } \tilde{\lambda}$ и, следовательно, $\tilde{\lambda}$ — автоморфизм поля $F/\mathbb{F}_q$, доказывающий, что $v_{Q_\infty}(\lambda(x)) = v_{Q_\infty}(\lambda(z)) = -2$, $v_{Q_\infty}(\lambda(y)) = -3$.

Сначала покажем, что $\lambda(x^i) = \lambda(x)^i$ для $i = 1, \dots, \alpha_{00}$. Выберем μ таким, что

$$\mu c \leq m < (\mu + 1)c \leq m + c.$$

Из условия теоремы $\deg((\lambda(x))_\infty) \leq c$ следует, что

$$\deg((\lambda(x)^2)_\infty) \leq 2c \leq m + c, \quad \text{поскольку } c \leq m.$$

Тогда $\lambda(x^2), \lambda(x)^2 \in \mathcal{L}((m + c)P_\infty)$, а по лемме 1 имеем

$$\lambda(x^2) = \lambda(x)^2 \quad \text{в } n > m + c \text{ точках.}$$

Продолжая рассуждения, заключаем:

$$\lambda(x^i) = \lambda(x)^i \quad \text{для } 1 \leq i \leq \mu.$$

Если $\mu = \alpha_{00}$, то получаем

$$-v_{P_\infty}(\lambda(x)) \leq \min \left\{ c; \left\lceil \frac{m}{\alpha_{00}} \right\rceil \right\}.$$

Иначе считаем, что $\mu < \alpha_{00}$, и тогда $x^{\mu+1} \in \mathcal{L}(mP_\infty)$. Так как $\deg(\lambda(x)^{\mu+1})_\infty \leq m + c$, то получаем

$$\lambda(x^{\mu+1}) = \lambda(x)^{\mu+1},$$

следовательно, $m \geq -v_{P_\infty}(\lambda(x^{\mu+1})) = -(\mu + 1)v_{P_\infty}(\lambda(x))$. Таким образом,

$$-v_{P_\infty}(\lambda(x)) \leq \frac{m}{\mu + 1} < c.$$

Применяя лемму 1 к $\mathcal{L}((m + c)P_\infty)$ и учитывая, что $-v_{P_\infty}(\lambda(x)^{\mu+2}) \leq (\mu + 2)\frac{m}{\mu + 1} = m + \frac{m}{\mu + 1} < m + c < n$, получаем

$$\lambda(x^{\mu+2}) = \lambda(x)^{\mu+1} \cdot \lambda(x).$$

Поскольку $-v_{P_\infty}(\lambda(x^{\mu+2})) \leq m$, то

$$-v_{P_\infty}(\lambda(x)) \leq \frac{m}{\mu + 2}.$$

Продолжая этот процесс, находим

$$-v_{P_\infty}(\lambda(x)) \leq \frac{m}{\alpha_{00}}.$$

Окончательно заключаем, что в любом случае

$$4 \leq -v_{P_\infty}(\lambda(x)) \leq \min \left\{ c; \left\lceil \frac{m}{\alpha_{00}} \right\rceil \right\}. \quad (3)$$

Отметим, что $\alpha_{00} = \left\lceil \frac{m}{4} \right\rceil \geq \frac{m-4+1}{4} = \frac{m-3}{4}$. Тогда $\left\lceil \frac{m}{\alpha_{00}} \right\rceil \leq \frac{4m}{m-3}$ и

$$-v_{P_\infty}(\lambda(x)) \leq \min \left\{ c; \frac{4m}{m-3} \right\}. \quad (4)$$

Учитывая, что $n > m+c$ и $\lambda(yx), \lambda(y)\lambda(x) \in \mathcal{L}((m+c)P_\infty)$, и снова применяя лемму 1, получаем

$$\lambda(yx) = \lambda(y)\lambda(x).$$

Переходя к нормированиям и учитывая, что изначально $\lambda(y) \in \mathcal{L}(mP_\infty)$, имеем $-v_{P_\infty}(\lambda(yx)) = -v_{P_\infty}(\lambda(y)) - v_{P_\infty}(\lambda(x)) \leq -v_{P_\infty}(\lambda(y))$. Следовательно,

$$-v_{P_\infty}(\lambda(y)) \leq m + v_{P_\infty}(\lambda(x)).$$

Рассматривая элемент $\lambda(yx^2)$, аналогичным образом заключаем, что $\lambda(yx^2) = \lambda(y)\lambda(x)^2$. Продолжая, получаем

$$\lambda(yx^s) = \lambda(y)\lambda(x)^s \text{ для } s = 0, \dots, \alpha_{10}.$$

Принимая во внимание, что элементы $y, xy, \dots, x^{\alpha_{10}}y$ входят в систему образующих пространства $\mathcal{L}(mP_\infty)$, и рассуждая по аналогии с (3), получаем

$$-v_{P_\infty}(\lambda(y)) \leq m - 4\alpha_{10}.$$

Поскольку $\alpha_{10} = \left\lceil \frac{m-3}{4} \right\rceil \geq \frac{m-3-4+1}{4} = \frac{m-6}{4}$, то

$$-v_{P_\infty}(\lambda(y)) \leq 6. \quad (5)$$

Аналогично рассуждаем для оценки величины $-v_{P_\infty}(\lambda(z))$. Поскольку $n > m+c$ и $\lambda(zx), \lambda(z)\lambda(x) \in \mathcal{L}((m+c)P_\infty)$, то $\lambda(zx) = \lambda(z)\lambda(x)$. Имеем

$$-v_{P_\infty}(\lambda(z)) \leq m + v_{P_\infty}(\lambda(x)).$$

Принимая во внимание, что элементы $z, xz, \dots, x^{\alpha_{01}}z$ входят в систему образующих пространства $\mathcal{L}(mP_\infty)$, получаем

$$-v_{P_\infty}(\lambda(z)) \leq m - 4\alpha_{01}.$$

Поскольку $\alpha_{01} = \left\lceil \frac{m-2}{4} \right\rceil \geq \frac{m-2-4+1}{4} = \frac{m-5}{4}$, то

$$-v_{P_\infty}(\lambda(z)) \leq 5. \quad (6)$$

Случай с элементами $yz, xyz, \dots, x^{\alpha_{11}}yz$ мы не рассматриваем, поскольку органичились рассмотрением уравнения (2), в котором они не фигурируют.

Поддействуем на определяющее уравнение λ , т.е. фактически осуществим замену x, y, z на $\lambda(x), \lambda(y), \lambda(z)$:

$$\begin{cases} (\lambda(z))^2(P'_i) = (\alpha_0 + \alpha_1\lambda(x) + \alpha_2(\lambda(x))^2 + \beta_0\lambda(y))(P'_i), \\ (\lambda(y))^2(P'_i) = ((\lambda(x))^3 + a\lambda(x) + b)(P'_i). \end{cases}$$

В первом уравнении функция $\lambda(z)^2$ в левой части имеет не более 10 полюсов (в силу условия (6)). Учитывая (5), (4) и неравенство треугольника (1), функция в правой части $\alpha_0 + \alpha_1\lambda(x) + \alpha_2(\lambda(x))^2 + \beta_0\lambda(y)$ имеет не более $\min\{8m/(m-3); 6\}$ полюсов. Поскольку равенство $8m/(m-3) = 6$ невозможно из-за условия $m \geq 4$, то окончательно эта функция имеет не более $8m/(m-3)$ полюсов.

Во втором уравнении функция $\lambda(y)^2$ в левой части имеет не более 12 полюсов, а функция $(\lambda(x))^3 + a\lambda(x) + b$ — не более $12m/(m-3)$ полюсов (в силу условий (5) и (4)).

Очевидно, что $\max\{m+c, 10, 8m/(m-3), 12, 12m/(m-3)\} = 12m/(m-3)$ при $m \geq 4$. Поскольку по построению $n > 12m/(m-3)$, можем применить лемму 1. Таким образом, функции в обеих частях двух уравнений совпадают. Следовательно, λ сохраняет определяющее уравнение исходного функционального поля кривой, откуда по теореме 3 элементы $\lambda(x), \lambda(y), \lambda(z)$ определяют эндоморфизм $\tilde{\lambda}$, такой, что $\tilde{\lambda} = \lambda|_{\mathcal{L}(mP_\infty)}$. А так как $x, y, z \in \text{Im } \tilde{\lambda}$, то $\tilde{\lambda}$ действует как автоморфизм соответственно $v_{P_\infty}(\lambda(x)) = v_{P_\infty}(\lambda(z)) = 2$ и $v_{P_\infty}(\lambda(y)) = 3$. ■

Используя теорему 4, можем определить группу автоморфизмов класса кодов, ассоциированных с функциональными полями оптимальных кривых рода три.

Теорема 5. Пусть $F/\mathbb{F}_p$ — функциональное поле оптимальной кривой рода три. Положим $m \geq 4$ и $D = \sum_{i=1}^n P_i$, где $P_i \in J$, P_i — точки степени один и $J \subseteq \mathbb{P}_F \setminus \{P_\infty\}$. Если $n > 12m/(m-3)$, то

$$\text{Aut}(\mathcal{C}_{\mathcal{L}}(D, mP_\infty)) \cong \text{Aut}_{D, mP_\infty}(F/\mathbb{F}_p).$$

Доказательство. Согласно теореме 1, группа $\text{Aut}_{D, mP_\infty}(F/\mathbb{F}_p)$ является подгруппой группы $\text{Aut}(\mathcal{C}_{\mathcal{L}}(D, mP_\infty))$. Покажем, при каких условиях достигается изоморфизм этих групп.

Рассмотрим $\pi \in \text{Aut}(\mathcal{C}_{\mathcal{L}}(D, mP_\infty))$. Поскольку $\mathcal{C}_{\mathcal{L}}(D, mP_\infty) = \mathcal{C}_{\mathcal{L}}(\pi(D), mP_\infty)$, в качестве π можем рассматривать отображение λ_π , ассоциированное с π и введённое в определении 9. Покажем, что λ_π является сужением автоморфизма $\tilde{\lambda} \in \text{Aut}_{D, mP_\infty}(F/\mathbb{F}_p)$.

По теореме 4 автоморфизм λ_π можно рассматривать как автоморфизм $\tilde{\lambda}$ функционального поля F на $\mathcal{L}(mP_\infty)$. Так как $\dim(mP_\infty) > 1$, то $\mathcal{L}(mP_\infty) \setminus \mathbb{F}_p \neq \emptyset$. Тогда существует функция $h \in \mathcal{L}(mP_\infty)$, такая, что h имеет полюс лишь в точке P_∞ и ни в какой другой точке. Имеем $\mathcal{L}(mP_\infty) = \tilde{\lambda}(\mathcal{L}(mP_\infty)) = \mathcal{L}(\tilde{\lambda}(mP_\infty))$. Кроме того, $\tilde{\lambda}(mP_\infty) = m\tilde{\lambda}(P_\infty)$ и, таким образом, $\tilde{\lambda}(P_\infty) = P_\infty$, иначе функция h будет иметь полюс в точке $\tilde{\lambda}(P)$, что невозможно по предположению. Следовательно, $\tilde{\lambda}(mP_\infty) = mP_\infty$.

Имеем $\mathcal{C}_{\mathcal{L}}(\pi(D), mP_\infty) = \mathcal{C}_{\mathcal{L}}(D, mP_\infty) = \mathcal{C}_{\mathcal{L}}(\tilde{\lambda}(D), \tilde{\lambda}(mP_\infty)) = \mathcal{C}_{\mathcal{L}}(\tilde{\lambda}(D), mP_\infty)$ и $\tilde{\lambda}(h) = \lambda(h)$ для всех $h \in \mathcal{L}(mP_\infty)$. Следовательно, $\tilde{\lambda}(h)(\tilde{\lambda}(P_i)) = \lambda(h)(\pi(P_i))$ для всех $h \in \mathcal{L}(mP_\infty)$ и $i = 1, \dots, n$.

Поскольку $F = \mathbb{F}_p(x, y, z)$, то если $P \in \mathbb{P}_F$ — точка степени один, значения $x(P), y(P)$ и $z(P)$ единственным образом определены в точке P . Так как $x, y, z \in \mathcal{L}(mP_\infty)$, то $x(\tilde{\lambda}(P_i)) = x(\pi(P_i))$, $y(\tilde{\lambda}(P_i)) = y(\pi(P_i))$, $z(\tilde{\lambda}(P_i)) = z(\pi(P_i))$ и, следовательно, $\tilde{\lambda}(P_i) = \pi(P_i)$ для $i = 1, \dots, n$. Получаем $\tilde{\lambda}(D) = \pi(D)$, откуда $\tilde{\lambda} \in \text{Aut}_{D, mP_\infty}(F/\mathbb{F}_p)$. ■

Приведём пример, ориентируясь на некоторые данные из [8].

Пример 1. Рассмотрим максимальную кривую, определённую над конечным полем $\mathbb{F}_{47}$:

$$\begin{cases} z^2 = 5 + 45x + 30x^2 + 10y, \\ y^2 = x^3 + x + 38. \end{cases}$$

Число её $\mathbb{F}_{47}$ -рациональных точек, удовлетворяющих границе Хассе — Вейля — Серра, равно 87. Отметим, что рациональные точки кривой соответствуют точкам степени один её функционального поля $F/\mathbb{F}_{47}$, поэтому в качестве дивизора D мы можем рассмотреть дивизор $D = P_1 + \dots + P_{87}$.

Для $m = 4$ рассмотрим дивизор $G = 4P_\infty$. Тогда, применяя теорему 5, получаем

$$\text{Aut}(\mathcal{C}(D, 4P_\infty)) \cong \text{Aut}_{D, 4P_\infty}(F/\mathbb{F}_p) \cong \text{Aut}_{\mathbb{F}_{47}}(C) \cong D_3.$$

ЛИТЕРАТУРА

1. Goppa V. D. Geometry and Codes. Kluwer Academic Publishers, 1988.
2. Stichtenoth H. On automorphisms of geometric Goppa codes // J. Algebra. 1990. V.130. P.113–121.
3. Xing C. Automorphism group of elliptic codes // Comm. Algebra. 1995. V.23. No.11. P.4061–4072.
4. Xing C. On automorphism groups of the Hermitian codes // IEEE Trans. Inform. Theory. 1995. V.41. No.6. P.1629–1635.
5. Малыгина Е. С. Исследование группы автоморфизмов кода, ассоциированного с оптимальной кривой рода три // Прикладная дискретная математика. Приложение. 2018. №11. С.115–117.
6. Stichtenoth H. Algebraic Function Fields and Codes. Springer Verlag, 1991.
7. Alekseenko E., Aleshnikov S., Markin N., and Zaytsev A. Optimal curves over finite fields with discriminant -19 // Finite Fields and Their Appl. 2011. V.17. Iss.4. P.350–358.
8. Alekseenko E. Explicit construction of optimal curves of genus three. PhD Thesis. 2016. http://iitp.ru/upload/content/1203/AES_disser.pdf

REFERENCES

1. Goppa V. D. Geometry and Codes. Kluwer Academic Publishers, 1988.
2. Stichtenoth H. On automorphisms of geometric Goppa codes. J. Algebra, 1990, vol.130, pp.113–121.
3. Xing C. Automorphism group of elliptic codes. Comm. Algebra, 1995, vol.23, no.11, pp.4061–4072.
4. Xing C. On automorphism groups of the Hermitian codes. IEEE Trans. Inform. Theory, 1995, vol.41, no.6, pp.1629–1635.
5. Malygina E. S. Issledovanie gruppy avtomorfizmov koda, assotsiirovannogo s optimal'noy krivoy roda tri [Investigation of automorphism group for code associated with optimal curve of genus three]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2018, no.11, pp.115–117. (in Russian)
6. Stichtenoth H. Algebraic Function Fields and Codes. Springer Verlag, 1991.
7. Alekseenko E., Aleshnikov S., Markin N., and Zaytsev A. Optimal curves over finite fields with discriminant -19 . Finite Fields and Their Appl., 2011, vol.17, iss.4, pp.350–358.
8. Alekseenko E. Explicit Construction of Optimal Curves of Genus Three. PhD Thesis, 2016. http://iitp.ru/upload/content/1203/AES_disser.pdf