АБСОЛЮТНО ПРОСТЫЕ ПРИМИАНЫ ТРИГОНАЛЬНЫХ КРИВЫХ

Ю.Г. ЗАРХИН

Посвящается В.А. Исковских в связи с его семидесятилетием

1. Введение

Как обычно, через $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ обозначаются кольцо целых чисел, поле рациональных чисел и поле комплексных чисел соответственно. Выберем примитивный кубический корень из единицы $\zeta_3 = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$. Пусть $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ - третье круговое поле и $\mathbb{Z}[\zeta_3] = \mathbb{Z}+\mathbb{Z}\cdot\zeta_3$ - кольцо всех его целых алгебраических чисел. Мы обозначаем через λ (главный) максимальный идеал $(1-\zeta_3)\cdot\mathbb{Z}[\zeta_3]$ кольца $\mathbb{Z}[\zeta_3]$.

Известно [11, Теорема 5 на с. 176] (см. также [5]), что для всех натуральных чисел m, отличных от двойки, существует m-мерное комплексное абелево многообразие с кольцом эндоморфизмов $\mathbb{Z}[\zeta_3]$. Доказательство Шимуры является чисто комплексно-аналитическим: грубо говоря, он работает с точками соответствующего пространства модулей, не принадлежащими счетному объединению подмногообразий положительной коразмерности. В этой работе мы обсуждаем геометрический подход к явному построению подобных абелевых многообразий, использующий якобианы, примианы и теорию Галуа.

Чтобы объяснить наш подход, начнем со следующих определений. Пусть $f(x) \in \mathbb{C}[x]$ - многочлен без кратных корней и степени $n \geq 4$. Пусть $C_{f,3}$ - гладкая проективная модель гладкой аффинной кривой $y^3 = f(x)$. Хорошо известно ([2], с. 401-402, [15], Предложение. 1 на с. 3359, [7], с. 148), что род $g(C_{f,3})$ кривой $C_{f,3}$ равен $n-1$ если 3 не делит n и $n-2$ если делит. В обоих случаях род $g(C_{f,3}) \geq 3$ *не* сравним с 2 по модулю 3.

Отображение $(x,y) \mapsto (x,\zeta_3 y)$ задает нетривиальный бирациональный автоморфизм $\delta_3 : C_{f,3} \to C_{f,3}$ периода 3. По функториальности, δ_3 индуцирует линейный оператор в пространстве дифференциалов первого рода

$$\delta_3^* : \Omega^1(C_{f,3}) \to \Omega^1(C_{f,3}).$$

Спектр этого оператора состоит из собственных чисел ζ_3^{-1} и ζ_3; если 3 не делит n, то их кратности равны $[n/3]$ и $[2n/3]$ соответственно [17].

Пусть $J(C_{f,3})$ - якобиан кривой $C_{f,3}$; это абелево многообразие размерности $g(C_{f,3})$. Обозначим через $\mathrm{End}(J(C_{f,3}))$ кольцо всех эндоморфизмов абелева многообразия $J(C_{f,3})$. По функториальности Альбанезе, δ_3 индуцирует автоморфизм якобиана $J(C_{f,3})$, который мы по-прежнему обозначаем через δ_3; известно ([11], с. 149, [14], с. 448) что $\delta_3^2+\delta_3+1=0$ в $\mathrm{End}(J(C_{f,3})$. Это дает нам вложение колец

$$\mathbb{Z}[\zeta_3] \cong \mathbb{Z}[\delta_3] \subset \mathrm{End}(J(C_{f,3})),\ \zeta_3 \mapsto \delta_3$$

([7, с. 149], [14], [9, с. 448]).

Если $f(x)$ нечетный многочлен нечетной степени n то на кривой $C_{f,3}$ имеется инволюция

$$\delta_2 : C_{f,3} \to C_{f,3}, (x,y) \mapsto (-x,-y),$$

коммутирующая с δ_3. (У этой инволюции ровно две неподвижные точки если n не делится на 3.) По функториальности Альбанезе, δ_2 индуцирует автоморфизм якобиана $J(C_{f,3})$, который мы по-прежнему обозначаем через δ_2 и который (по-прежнему) коммутирует с автоморфизмом δ_3 якобиана $J(C_{f,3})$. Имеем $\delta_2^2 = 1$ в $\mathrm{End}(J(C_{f,3}))$.

Пусть K - подполе поля $\mathbb{C}$, содержащее $\sqrt{-3}$ и все коэффициенты многочлена $f(x)$, т.е.,

$$f(x) \subset K[x] \subset \mathbb{C}[x].$$

Пусть $\mathfrak{R}_f \subset \mathbb{C}$ - множество всех корней многочлена $f(x)$ и $K(\mathfrak{R}_f)$ - поле разложения многочлена $f(x)$ над полем K. Ясно, что поле $K(\mathfrak{R}_f)$ - конечное расширение Галуа поля K. Обозначим через $\mathrm{Gal}(f)$ (конечную) группу Галуа $\mathrm{Gal}(K(\mathfrak{R}_f)/K)$. Можно рассматривать $\mathrm{Gal}(f)$ как определенную подгруппу перестановок в группе $\mathrm{Perm}(\mathfrak{R}_f)$ всех перестановок множества $\mathfrak{R}_f$. Если мы (выберем порядок на множестве $\mathfrak{R}_f$, т.е.,) обозначим корни многочлена $f(x)$ через $\{\alpha_1, \dots, \alpha_n\}$, то мы получим изоморфизм между группой $\mathrm{Perm}(\mathfrak{R}_f)$ и полной симметрической группой group $\mathbf{S}_n$, а $\mathrm{Gal}(f)$ окажется определенной подгруппой в $\mathbf{S}_n$.

В работах [16, 19] доказано, что если $\mathrm{Gal}(f) = \mathbf{S}_n$ то

$$\mathrm{End}(J(C_{f,3})) = \mathbb{Z}[\delta_3] \cong \mathbb{Z}[\zeta_3].$$

В частности, это позволяет нам явно построить g-мерные главнополяризованые абелевы многообразия с кольцом эндоморфизмов $\mathbb{Z}[\zeta_3]$ для всех $g \geq 3$, для которых 3 не делит divide $g-2$. Например, если $f(x) = x^{g+1} - x - 1$ то $J(C_{f,3})$ - g-мерное главнополяризованое абелево многообразие, то $\mathrm{End}(J(C_{f,3})) = \mathbb{Z}[\zeta_3]$. (Известно [10, с. 42], что группа Галуа многочлена $x^n - x - 1$ над $\mathbb{Q}$ совпадает с $\mathbf{S}_n$ для всех натуральных n.)

Цель этой работы - дать *явную* конструкцию m-мерных главнополяризованых абелевых многообразий с кольцом эндморфизмов $\mathbb{Z}[\zeta_3]$ для всех нечетных $m \geq 5$, сравнимых с 2 по модулю 3. Мы построим их (используя нечетные $f(x)$ степени $n = 2m+1$) как антиинвариантную часть (многобразие Прима) якобиана $J(C_{f,3})$ относительно инволюции δ_2, предполагая, что $\mathrm{Gal}(f)$ совпадает с группой Вейля $\mathbb{W}(\mathbb{D}_m)$ системы корней $\mathbb{D}_m$ в следующем смысле. Поскольку $f(x)$ нечетен и без кратных корней, найдутся m различных ненулевых корня $\{\beta_1, \dots, \beta_m\}$ многочлена $f(x)$, такие, что ($\beta_i \neq \pm\beta_j$ если $i \neq j$ и) $\mathfrak{R}_f$ совпадает с $\{0\} \cup \{\pm\beta_1, \dots, \pm\beta_m\} \subset \bar{K}$. Тогда можно определить $\mathbb{W}(\mathbb{D}_m)$ как группу всех перестановок множества $\mathfrak{R}_f$, имеющих вид

$$0 \mapsto 0,\ \beta_i \mapsto \epsilon_i \beta_{s(i)},\ -\beta_i \mapsto -\epsilon_i \beta_{s(i)}$$

где $s \in \mathbf{S}_m$ - произвольная перестановка, а знаки $\epsilon_i = \pm 1$ удовлетворяют условию $\prod_{i=1}^m \epsilon_i = 1$. Рассмотрим m-мерное векторное пространство над $\mathbb{F}_3$ всех *нечетных*функций

$$V_f^- := \{\phi : \mathfrak{R}_f \to \mathbb{F}_3 \mid \phi(-\alpha) = -\phi(\alpha)\ \forall \alpha \in \mathfrak{R}_f\},$$

снабженное естественной структурой модуля Галуа.

Нашим основным результатом следующее утверждение.

Теорема 1.1. *Пусть k - неотрицательное целое число, $m = 6k + 5 \geq 5, n = 2m+1 = 12k+11$. Пусть $f(x)$ - нечетный многочлен степени n и без кратных корней. Тогда:*

(i) (1) (A) *Образ $P(C_{f,3}) := (1 - \delta_2)J(C_{f,3})$ является m-мерным δ_3-инвариантным абелевым подмногообразием в $J(C_{f,3})$. В частности, вложение $\mathbb{Z}[\delta_3] \subset \mathrm{End}(J(C_{f,3}))$ индуцирует вложение*

$$\mathbb{Z}[\zeta_3] \cong \mathbb{Z}[\delta_3] \hookrightarrow \mathrm{End}(P(C_{f,3})).$$

(B) *Если ограничить каноническую главную поляризацию якобиана $J(C_{f,3})$ на его абелево подмногообразие $P(C_{f,3})$, то индуцированная поляризация является главной поляризацией на $P(C_{f,3})$, умноженной на два, и эта главная поляризация является δ_3-инвариантной.*

(C) *Главнополяризованное абелево многообразие $P(C_{f,3})$ не изоморфно канонически поляризованному якобиану какой-либо гладкой проективной кривой.*

(2) *По функториальности, δ_3 индуцирует линейный оператор*

$$\delta_{3,P}^* : \Omega^1(P(C_{f,3})) \to \Omega^1(P(C_{f,3}))$$

в пространстве дифференциалов первого рода на $P(C_{f,3})$. Его спектр состоит из собственных чисел ζ_3^{-1} кратности $2k + 1$ и ζ_3 кратности $4k + 4$ соответственно.

(ii) *Пусть K - подполе в $\mathbb{C}$, содержащее $\sqrt{-3}$ и все коэффициенты многочлена $f(x)$. Тогда:*

(a) *Абелево многообразие $P(C_{f,3})$ и его автоморфизм δ_3 определены над K. Вдобавок, подмодуль Галуа $P(C_{f,3})^{\delta_3}$ всех δ_3-инвариантов в $P(C_{f,3})(\bar{K})$ канонически изоморфен модулю Галуа V_f^-.*

(b) *Предположим дополнительно, что группа $\mathrm{Gal}(f)$ совпадает с $\mathbb{W}(\mathbb{D}_m)$. Тогда:*

(b1) $\mathrm{End}(P(C_{f,3})) = \mathbb{Z}[\zeta_3]$. *В частности, $P(C_{f,3})$ - абсолютно простое абелево многообразие.*

(b2) *Комплексное абелево многообразие $P(C_{f,3})$ не изоморфно ни якобиану какой-либо гладкой проективной кривой ни произведению якобианов гладких проективных кривых (даже если не учитывать поляризации).*

Пример 1.2. Пусть $m = 5$ и $f(x) := x(x^{10}-x^2-1)$. Можно проверить (см. Пример 2.3 below), что группа Галуа многочлена $f(x)$ над $K = \mathbb{Q}(\sqrt{-3})$ совпадает с $\mathbb{W}(\mathbb{D}_5)$. Отсюда вытекает, что

$$\mathrm{End}(P(C_{f,3})) = \mathbb{Z}[\zeta_3].$$

Замечание 1.3. При $m = 5$ пятимерные многообразия Прима $P(C_{f,3})$ реализуются как промежуточные якобианы некоторых трехмерных кубик [3]. (См. также [20].)

Замечание 1.4. Полный список (обобщенных) многообразий Прима, которые изоморфны (как главнополяризованные абелевы многообразия) якобианам гладких проективных кривых или их произведениям был получен В.В. Шокуровым [13, 14]. При доказательстве Теоремы 1.1(b2) мы используем другой

подход, основанный на изучении действия автоморфизма периода 3 на дифференциалы первого рода [20].

Статья организована следующим образом. В параграфе 2 мы обсуждаем пермутационные модули, связанные с группами Галуа нечетных многочленов. В параграфе 3 мы изучаем тригональные якобианы и примианы и доказываем основной результат.

Я признателен В.В. Шокурову за полезные обсуждения. Моя особая благодарность - доктору Арсену Елкину, выполнившему вычисления с системой MAGMA, связанные с Примером 2.3.

2. Группы Галуа нечетных полиномов м пермутационные модули

Пусть K - поле нулевой характеристики , $\bar{K}$ - его алгебраическое замыкание и $\mathrm{Gal}(K) = \mathrm{Aut}(\bar{K}/K)$ - его абсолютная группа Галуа. Пусть $\gamma \in K$ - примитивный кубический корень из единицы.

2.1. Группы Галуа нечетных полиномов. Пусть $n = 12k+11$ - натуральное число, сравнимое с 11 по модулю 12, $f(x) \in K[x]$ - *нечетный* многочлен степени n *без кратных корней* и с *ненулевым* постоянным членом. Положим $m = 6k + 5$. Тогда найдутся m различных ненулевых корней $\{\beta_1, \dots, \beta_m\}$ многочлена $f(x)$, такие, что the n-элементное множество $\mathfrak{R}_f$ всех корней многочлена $f(x)$ совпадает с $\{0\} \cup \{\pm\beta_1, \dots, \pm\beta_m\} \subset \bar{K}$ of all roots of $f(x)$. Ясно, что множество $\mathfrak{R}_f$ переводится в себя автоморфизмами Галуа. Через $\mathrm{Perm}(\mathfrak{R}_f)$ обозначается группа всех перестановок n-элементного множества $\mathfrak{R}_f$. Пусть $\mathrm{Gal}(f)$ - образ группы $\mathrm{Gal}(K)$ в $\mathrm{Perm}(\mathfrak{R}_f)$ относительно естественного действия группы Галуа на корни многочлена $f(x)$. Если $K(\mathfrak{R}_f)$ - поле разложения многочлена $f(x)$, получаемое присоединением к K всех элементов множества $\mathfrak{R}_f$, то $K(\mathfrak{R}_f)/K$ - конечное расширение Галуа и группа $\mathrm{Gal}(f)$ канонически изоморфна группе Галуа $\mathrm{Gal}(K(\mathfrak{R}_f)/K)$. Пусть $\mathrm{Perm}_0(\mathfrak{R}_f)$ - подгруппа группы $\mathrm{Perm}(\mathfrak{R}_f)$, которая состоит из всех перестановок вида

$$0 \mapsto 0,\ \beta_i \mapsto \epsilon_i \beta_{s(i)},\ -\beta_i \mapsto -\epsilon_i \beta_{s(i)}$$

где $s \in \mathbf{S}_m$ - произвольная перестановка, а $\epsilon_i = \pm 1$. Ясно, что

$$\mathrm{Gal}(f) \subset \mathrm{Perm}_0(\mathfrak{R}_f) \subset \mathrm{Perm}(\mathfrak{R}_f).$$

Обозначим через $\mathbb{W}(\mathbb{D}_m)$ подгруппу индекса 2 группы $\mathrm{Perm}_0(\mathfrak{R}_f)$, элементы которой характеризуются условием $\prod_{i=1}^m \epsilon_i = 1$. Имеем

$$\mathbb{W}(\mathbb{D}_m) \subset \mathrm{Perm}_0(\mathfrak{R}_f) \subset \mathrm{Perm}(\mathfrak{R}_f).$$

Поскольку 0 - простой корень для $f(x)$, то мы имеем $f(x) = x \cdot h(x)$ где $h(x)$ - *четный* многочлен четной степени $2m$, а множество всех его корней $\mathfrak{R}_h$ совпадает с $\{\pm\beta_1, \dots, \pm\beta_m\}$; в частности, $h(0) \neq 0$.

Замечание 2.2. Ясно, что $(\prod_{i=1}^m \beta_i)^2 = -h(0)$ (напомним, что m нечетно). Отсюда вытекает, что $\mathrm{Gal}(f) = \mathrm{Gal}(h) \subset \mathbb{W}(\mathbb{D}_m)$ если и только если $-h(0)$ квадрат в K.

Пример 2.3. Пусть

$$m = 5, h(x) = x^{10} - x^2 - 1 \in \mathbb{Q}[x], f(x) = x \cdot h(x) = x(x^{10} - x^2 - 1).$$

Поскольку $1 = -h(0)$ квадрат в $\mathbb{Q}$, группа Галуа $\mathrm{Gal}(h/\mathbb{Q})$ многочлена $h(x)$ над $\mathbb{Q}$ является подгруппой в $\mathbb{W}(\mathbb{D}_5)$. Используя систему Magma [1], можно

получить, что порядок группы $\mathrm{Gal}(h/\mathbb{Q})$ равен $2^4 \cdot 5!$. Поскольку порядок группы $\mathbb{W}(\mathbb{D}_5)$ также равен $2^4 \cdot 5!$, мы заключаем, что $\mathrm{Gal}(h/\mathbb{Q}) = \mathbb{W}(\mathbb{D}_5)$. Можно проверить, что коммутант $G_1 := (\mathbb{W}(\mathbb{D}_5), \mathbb{W}(\mathbb{D}_5))$ - *совершенная* (нормальная) подгруппа индекса 2 в $W(\mathbb{D}_5)$. Отсюда вытекает, что поле разложения $\mathbb{Q}(\mathfrak{R}_h)$ для $h(x)$ над $\mathbb{Q}$ содержит ровно одно квадратичное подполе. Чтобы определить это подполе, заметим, что если $\{\pm\beta_1, \dots, \pm\beta_5\}$ - множество всех корней многочлена $h(x) = x^{10} - x^2 - 1$ то $\{\beta_1^2, \dots \beta_5^2\}$ - множество всех корней многочлена $x^5 - x - 1$. Используя систему Magma [1], получаем, что дискриминант многочлена $x^5 - x - 1$ равен 19×151 и следовательно, $\mathbb{Q}(\mathfrak{R}_h)$ содержит $\mathbb{Q}(\sqrt{19 \times 151})$. Отсюда вытекает, что $\mathbb{Q}(\mathfrak{R}_h)$ *не* содержит $K = \mathbb{Q}(\sqrt{-3})$ и следовательно, $\mathbb{Q}(\mathfrak{R}_h)$ и K линейно разделены над $\mathbb{Q}$. Отсюда вытекает, что группа Галуа многочлена $h(x)$ над K также совпадает с $\mathbb{W}(\mathbb{D}_5)$ и следовательно, группа Галуа многочлена $f(x)$ над K также совпадает с $\mathbb{W}(\mathbb{D}_5)$.

Определение 2.4. Пусть $\mathrm{Perm}(\mathfrak{R}_h)$ - группа всех перестановок $2m$-элементного множества $\mathfrak{R}_h$. Пусть $\mathcal{G}$ - подгруппа перестановок в $\mathbf{S}_m$. Обозначим через $2^m \cdot \mathcal{G} \subset \mathrm{Perm}(\mathfrak{R}_h)$ подгруппу, состоящую из всех перестановок вида

$$(s; \epsilon_1, \dots, \epsilon_m) : \beta_i \mapsto \epsilon_i \beta_{s(i)}, \ -\beta_i \mapsto -\epsilon_i \beta_{s(i)}$$

где

$$s \in \mathcal{G}, \ \epsilon_i = \pm 1.$$

Обозначим через $2^{m-1} \cdot \mathcal{G}$ подгруппу индекса 2 группы $2^m \cdot \mathcal{G}$, элементы которой характеризуются условием $\prod_{i=1}^m \epsilon_i = 1$.

Пример 2.5.

(i) Группа $2^m \cdot \{1\}$ совпадает с группой всех перестановок вида

$$\beta_i \mapsto \epsilon_i \beta_i, \ -\beta_i \mapsto -\epsilon_i \beta_i$$

где $\epsilon_i = \pm 1$, в то время как $2^{m-1} \cdot \{1\}$ отвечает ее подгруппе индекса 2, элементы которой характеризуются условием $\prod_{i=1}^m \epsilon_i = 1$. Группы $2^m \cdot \{1\}$ и $2^{m-1} \cdot \{1\}$ коммутативны и имеют экспоненту 2, их порядки - 2^m и 2^{m-1} соответственно.

(ii) Отождествим $\mathrm{Perm}(\mathfrak{R}_h)$ со стабилизатором (корня) 0 в $\mathrm{Perm}(\mathfrak{R}_f)$. Тогда группа $2^m \cdot \mathbf{S}_m$ совпадает с $\mathrm{Perm}_0(\mathfrak{R}_f)$, а (под)группа $2^{m-1} \cdot \mathbf{S}_m$ совпадает с $\mathbb{W}(\mathbb{D}_m)$.

Замечание 2.6. Ясно, что естественное отображение $(s; \epsilon_1, \dots, \epsilon_m) \mapsto s$ задает сюръективные гомоморфизмы групп

$$\kappa_h^0 : 2^m \cdot \mathcal{G} \twoheadrightarrow \mathcal{G}, \ \kappa_h : 2^{m-1} \cdot \mathcal{G} \twoheadrightarrow \mathcal{G},$$

w ядра которых суть группы $2^m \cdot \{1\}$ и $2^{m-1} \cdot \{1\}$ соответственно.

Замечания 2.7. Предположим, что найдется группа подстановок $\mathcal{G} \subset \mathbf{S}_m$, такая, что $\mathrm{Gal}(h) = 2^{m-1} \cdot \mathcal{G}$. Тогда:

(i) Ядро сюръективного гомоморфизма $\kappa_h : \mathrm{Gal}(h) = 2^{m-1} \cdot \mathcal{G} \twoheadrightarrow \mathcal{G}$ - коммутативная (нормальная) подгруппа $2^{m-1} \cdot \{1\}$ экспоненты 2.

(ii) Пусть G_1 *нормальная* подгруппа группы $\mathrm{Gal}(h)$ *нечетного индекса* r. Тогда G_1 содержит $2^{m-1} \cdot \{1\}$ и сюръективность гомоморфизма κ_h влечет за собой то, что

$$\kappa_h(G_1) \cong G_1/(2^{m-1} \cdot \{1\})$$

- нормальная подгруппа индекса r в $\mathcal{G}$. Отсюда вытекает, что если группа $\mathcal{G}$ не содержит нормальную подгруппу нечетного индекса (за исключением самой $\mathcal{G}$) то группа $\mathrm{Gal}(h)$ также не содержит нормальную подгруппу нечетного индекса (за исключением самой $\mathrm{Gal}(h)$).

(iii) (1) Если $\mathcal{G}$ транзитивная подгруппа в $\mathbf{S}_m$ то $2^{m-1} \cdot \mathcal{G}$ транзитивная подгруппа в $\mathrm{Perm}(\mathfrak{R}_h)$. Это означает, что $\mathrm{Gal}(h)$ - транзитивная подгруппа в $\mathrm{Perm}(\mathfrak{R}_h)$, т.е., многочлен $h(x)$ неприводим над K.

(2) Предположим, что $\mathcal{G}$ дважды транзитивная подгруппа в $\mathbf{S}_m$ и пусть $\mathcal{G}_1$ - стабилизатор элемента 1 в $\mathcal{G}$. Тогда у $\mathcal{G}_1$ имеется ровно две орбиты в in $\{1, \dots, m\}$: а именно, $\{1\}$ и все остальное. Пусть $\mathrm{Gal}(h)_1$ - стабилизатор корня β_1 в $\mathrm{Gal}(h)$. Тогда легко убедиться в том, что у группы $\mathrm{Gal}(h)_1$ ровно три орбиты в $\mathfrak{R}_h$: а именно, $\{\beta_1\}$, $\{-\beta_1\}$ и все остальное.

2.8. Пермутационные модули. Пусть V_f - $2m$-мерное векторное пространство над $\mathbb{F}_3$ всех функций $\phi : \mathfrak{R}_f \to \mathbb{F}_3$, удовлетворяющих условию $\sum_{\alpha \in \mathfrak{R}_f} \phi(\alpha) = 0$. Пространство V_f снабжено естественной структурой модуля Галуа, индуцированное действием группы Галуа на множество $\mathfrak{R}_f$.

Пусть $\mathbb{F}_3^{\mathfrak{R}_h}$ - $2m$-мерное векторное пространство над $\mathbb{F}_3$ всех функций $\phi : \mathfrak{R}_h \to \mathbb{F}_3$. Пространство $\mathbb{F}_3^{\mathfrak{R}_h}$ снабжено естественной структурой модуля Галуа. Обозначим через $1_{\mathfrak{R}_h}$ постоянную (Галуа-инвариантную) функцию 1.

Отображение, сопоставляющее любой $\mathbb{F}_3$-значной функции на $\mathfrak{R}_f$ ее ограничение на $\mathfrak{R}_h$ задает изоморфизм модулей Галуа $V_f \to \mathbb{F}_3^{\mathfrak{R}_h}$. (Можно продолжить любую функцию ϕ на $\mathfrak{R}_h$ до функции на $\mathfrak{R}_f = \{0\} \cup \mathfrak{R}_h$, полагая

$$\phi(0) := -\sum_{\alpha \in \mathfrak{R}_h} \phi(\alpha).)$$

Модуль Галуа V_f расщепляется в прямую сумму модулей Галуа четных и нечетных функций

$$V_f = V_f^- \oplus V_f^+$$

где

$$V_f^+ = \{\phi : \mathfrak{R}_f \to \mathbb{F}_3, \sum_{\alpha \in \mathfrak{R}_f} \phi(\alpha) = 0,\ \phi(\alpha) = \phi(-\alpha)\ \forall \alpha\},$$

$$V_f^- = \{\phi : \mathfrak{R}_f \to \mathbb{F}_3,\ \phi(\alpha) = -\phi(\alpha)\ \forall \alpha\}.$$

(Сумма всех значений нечетной функции всегда равна нулю.) Ясно, что $\phi(0) = 0$ для всех $\phi \in V_f^-$. Отсюда вытекает, что

$$\dim_{\mathbb{F}_3}(V_f^-) = m.$$

Лемма 2.9. *Предположим, что существует дважды транзитивная группа перестановок $\mathcal{G} \subset \mathbf{S}_m$, такая, что $\mathrm{Gal}(h) = 2^{m-1} \cdot \mathcal{G}$. Тогда $\mathrm{End}_{\mathrm{Gal}(K)}(V_f^-) = \mathbb{F}_3$.*

Доказательство. Согласно Замечанию 2.7(iii)(1), группа $\mathrm{Gal}(h)$ транзитивно действует на множество $\mathfrak{R}_h$.

Пусть W_h^+ and W_h^- - подпространства пространства $\mathbb{F}_3^{\mathfrak{R}_h}$, состоящие из всех четных и нечетных функций соответственно. Ясно, что оба подпространства являются подмодулями Галуа в $\mathbb{F}_3^{\mathfrak{R}_h}$, а также

$$W_h^- \oplus W_h^+ = \mathbb{F}_3^{\mathfrak{R}_h}.$$

Также ясно, что модули Галуа W_h^- и V_f^- изоморфны. Поэтому, нам достаточно проверить, что

$$\mathrm{End}_{\mathrm{Gal}(K)}(W_h^-) = \mathbb{F}_3.$$

Для этого заметим, что натуральное число $\#(\mathfrak{R}_h) = 2m = n-1 = 12k+10$ *не* делится на 3. Отсюда вытекает, что подмодуль $\mathbb{F}_3 \cdot 1_{\mathfrak{R}_h}$ постоянных функций является прямым слагаемым в W_h^+, а модуль Галуа $\mathbb{F}_3^{\mathfrak{R}_h}$ расщепляется в прямую сумму модулей Галуа

$$\mathbb{F}_3^{\mathfrak{R}_h} = W_h^- \oplus W_h^+ = W_h^- \oplus \mathbb{F}_3 \cdot 1_{\mathfrak{R}_h} \oplus W_h^{+,0}$$

где $W_h^{+,0}$ - (под)модуль Галуа всех четных функций, для которых сумма всех значений равна нулю. Ясно, что

$$\dim_{\mathbb{F}_3}\mathrm{End}_{\mathrm{Gal}(K)}(\mathbb{F}_3^{\mathfrak{R}_h}) \geq$$

$$\dim_{\mathbb{F}_3}\mathrm{End}_{\mathrm{Gal}(K)}(W_h^-) + \dim_{\mathbb{F}_3}\mathrm{End}_{\mathrm{Gal}(K)}(\mathbb{F}_3 \cdot 1_{\mathfrak{R}_h}) + \dim_{\mathbb{F}_3}\mathrm{End}_{\mathrm{Gal}(K)}(W_h^{+,0}) \geq$$

$$\dim_{\mathbb{F}_3}\mathrm{End}_{\mathrm{Gal}(K)}(W_h^-) + 1 + 1.$$

Таким образом, если мы докажем, что $\dim_{\mathbb{F}_3}\mathrm{End}_{\mathrm{Gal}(K)}(\mathbb{F}_3^{\mathfrak{R}_h}) = 3$ то доказательство будет завершено. Поскольку образ группы $\mathrm{Gal}(K)$ в $\mathrm{Aut}_{\mathbb{F}_3}(\mathbb{F}_3^{\mathfrak{R}_h})$ совпадает с

$$\mathrm{Gal}(h) \subset \mathrm{Perm}(\mathfrak{R}_h) \subset \mathrm{Aut}_{\mathbb{F}_3}(\mathbb{F}_3^{\mathfrak{R}_h}),$$

мы имеем равенство.

$$\mathrm{End}_{\mathrm{Gal}(K)}(\mathbb{F}_3^{\mathfrak{R}_h}) = \mathrm{End}_{\mathrm{Gal}(h)}(\mathbb{F}_3^{\mathfrak{R}_h}).$$

Таким образом, для доказательства нашей Леммы достаточно убедиться в том, что

$$\dim_{\mathbb{F}_3}(\mathrm{End}_{\mathrm{Gal}(h)}(\mathbb{F}_3^{\mathfrak{R}_h})) = 3.$$

Согласно Лемме 7.1 книги [6], размерность $\dim_{\mathbb{F}_3}(\mathrm{End}_{\mathrm{Gal}(h)}(\mathbb{F}_3^{\mathfrak{R}_h}))$ совпадает с числом орбит в множестве $\mathfrak{R}_h$ относительно действия стабилизатора любого фиксированного корня многочлена $h(x)$ в $\mathrm{Gal}(h)$. Но это число орбит равно тройке (см. Замечание 2.7(iii)). Доказательство окончено. □

3. Циклические накрытия, якобианы и примианы

Если X - абелево многообразие над $\bar{K}$ то через $\mathrm{End}(X)$ обозначается кольцо всех его $\bar{K}$-эндоморфизмов, а через $\mathrm{End}^0(X)$ - соответствующая $\mathbb{Q}$-алгебра $\mathrm{End}(X) \otimes \mathbb{Q}$. Если X определена над K то через $\mathrm{End}_K(X)$ обозначается кольцо всех его K-эндоморфизмов.

Как и выше $f(x) = x \cdot h(x) \in K[x]$ - нечетный многочлен нечетной степени $n = 2m+1 = 12k+11$ и без кратных корней. Мы сохраняем все обозначения предыдущего параграфа.

3.1. Тригональные кривые. Здесь и далее мы предполагаем, что поле K содержит $\sqrt{-3}$. Рассмотрим гладкую проективную кривую $C_{f,3}$, являющуюся моделью аффинной тригональной кривой

$$y^3 = f(x);$$

ее род равен $n-1 = 12k+10$. На кривой $C_{f,3}$ действуют коммутирующие периодические автоморфизмы

$$\delta_2 : (x,y) \mapsto (-x,-y)$$

и

$$\delta_3 : (x, y) \mapsto (x, \gamma y,)$$

имеющие период 2 и 3 соответственно.

Регулярное отображение кривых

$$\pi : C_{f,3} \to \mathbb{P}^1,\ (x, y) \mapsto x$$

имеет степень 3 и разветвлено в точности в 0, $2m$-элементном множестве $\{\alpha \mid \alpha \in \mathfrak{R}_f\}$ и ∞. (Отметим, что 3 *не* делит $2m + 1$.) Ясно, что все точки ветвления отображения π в $C_{f,3}$ являются δ_3-инвариантными. Мы позволим себе обозначить $\pi^{-1}(\infty)$ через ∞. Положим

$$B = \pi^{-1}(\mathfrak{R}_f) = \{(\alpha, 0) \mid \alpha \in \mathfrak{R}_f\} \subset C(\bar{K}).$$

Ясно, что все элементы множества B являются δ_3-инвариантными. С другой стороны, если $P = (\alpha, 0) \in B$ то $\delta_2(P) = (-\alpha, 0) \in B$.

У автоморфизма $\delta_2 : C_{f,3} \to C_{f,3}$ ровно две неподвижные точки, а именно, $\pi^{-1}(0)$ и $\pi^{-1}(\infty)$. Легко проверяется, что фактор $\tilde{C}_{f,3} = C_{f,3}/(1, \delta_2)$ - гладкая (неприводимая) проективная кривая (сравните с Леммой 1.2, ее доказательством и Следствием 1.3 в работе [20]) и естественное регулярное отображение $C_{f,3} \to \tilde{C}_{f,3}$ является двойным накрытием, разветвленным ровно в двух точках, а именно в образах точек $\pi^{-1}(0)$ and $\pi^{-1}(\infty)$. Из формулы Гурвица вытекает, что род кривой $\tilde{C}_{f,3}$ равен m.

Поскольку

$$[n/3] = 4k + 3,\ [2n/3] = 8k + 7,$$

из результатов работ [16] и [17, Замечания 3.5 and 3.7] вытекает, что $(n-1)$-мерное векторное пространство $\Omega^1(C_{f,3})$ (над $\bar{K}$) дифференциалов первого рода на $C_{f,3}$ допускает в качестве базиса множество

$$\left\{ x^i \frac{dx}{y},\ 0 \le i \le 4k + 2;\ x^j \frac{dx}{y^2},\ 0 \le j \le 8k + 6 \right\}.$$

Если

$$\delta_2^* : \Omega^1(C_{f,3}) \to \Omega^1(C_{f,3}),\ \delta_3^* : \Omega^1(C_{f,3}) \to \Omega^1(C_{f,3})$$

- автоморфизмы, индуцированные δ_2 и δ_3 соответственно, то

$$\delta_3^*(x^i \frac{dx}{y}) = \gamma^{-1} x^i \frac{dx}{y},\ \delta_3^*(x^j \frac{dx}{y^2}) = \gamma^{-2} x^j \frac{dx}{y^2} = \gamma x^j \frac{dx}{y^2},$$

$$\delta_2^*(x^i \frac{dx}{y}) = (-1)^i x^i \frac{dx}{y},\ \delta_2^*(x^j \frac{dx}{y^2}) = (-1)^{j+1} x^j \frac{dx}{y^2};$$

в частности, этот базис состоит из собственных векторов линейных операторов δ_2^* and δ_3^*. Отсюда вытекает, что подпространство $\Omega^1(C_{f,3})^-$ всех δ_2-антиинвариантов имеет размерность m и допускает в качестве базиса множество

$$\left\{ x^{2i+1} \frac{dx}{y},\ 0 \le i \le 2k;\ x^{2j} \frac{dx}{y^2}\ 0 \le j \le 4k + 3 \right\}.$$

3.2. Тригональные якобианы. Пусть $J(C_{f,3})$ - якобиан кривой $C_{f,3}$: это $(n-1)$-мерное абелево многообразие, определенное над K. По функториальности Альбанезе, δ_2 и δ_3 индуцируют K-автоморфизмы якобиана $J(C_{f,3})$, которые мы по-прежнему обозначаем через δ_2 и δ_3 соответственно. Имеем

$$\delta_2^2 = 1,\ \delta_3^2 + \delta_3 + 1 = 0$$

где все равенства имеют место в кольце $\mathrm{End}(J(C_{f,3}))$. Последнее равенство позволяет определить вложение

$$\mathbb{Z}[\zeta_3] \hookrightarrow \mathrm{End}_K(J(C_{f,3})),\ \zeta_3 \mapsto \delta_3$$

кругового кольца $\mathbb{Z}[\mu_3]$ в кольцо всех K-эндоморфизмов абелева многообразия $J(C_{f,3})$.

Пусть $j : C_{f,3} \hookrightarrow J(C_{f,3})$ - каноническое вложение кривой $C_{f,3}$ в ее якобиан, нормализованное условием $j(\infty) = 0$, т.е., j переводит точку $P \in C_{f,3}(\bar{K})$ в класс линейной эквивалентности дивизора $(P) - (\infty)$. Ясно, что j является δ_3-эквивариантным и δ_2-эквивариантным.

Напомним описание (под)модуля Галуа $J(C_{f,3})^{\delta_3}$ всех δ_3-инвариантов в $J(C_{f,3})(\bar{K})$. Модули Галуа V_f и $J(C_{f,3})^{\delta_3}$ канонически изоморфны [9] (см. также [18]). А именно, пусть

$$\mathbb{Z}_B^0 = \{\sum_{P\in B} a_P(P) \mid a_P \in \mathbb{Z},\ \sum_{P\in B} a_P = 0\}$$

- группа всех дивизоров нулевой степени на кривой $C_{f,3}$ с носителем в B. Свободная коммутативная группа $\mathbb{Z}_B^0$ обладает естественной структурой модуля Галуа. Ясно, что модуль Галуа $\mathbb{Z}_B^0/3\mathbb{Z}_B^0$ канонически изоморфен модулю V_f: дивизор $\sum_{P\in B} a_P(P)$ задает функцию $\alpha \mapsto a_P \mod 3$ где $P = (\alpha, 0)$. Поскольку множество B является δ_2-инвариантным, отображение

$$D_2 : \sum_{P\in B} a_P(P) \mapsto \sum_{P\in B} a_P(\delta_2 P)$$

- автоморфизм модуля Галуа $\mathbb{Z}_B^0$, индуцирующий автоморфизм модуля Галуа $\mathbb{Z}_B^0/3\mathbb{Z}_B^0 = V_f$, который переводит функцию $\alpha \to \phi(\alpha)$ в функцию $\alpha \to \phi(-\alpha)$. (Мы сохраняем обозначение D_2 для этого автоморфизма модуля Галуа V_f.) Заметим, что

$$V_f^- = (1 - D_2)V_f,\ V_f^+ = (1 + D_2)V_f$$

(напомним, что V_f - векторное пространство над $\mathbb{F}_3$.) Другими словами, V_f^+ и V_f^- - собственные подпространства оператора D_2, отвечающие собственным значениям 1 и -1 соответственно.

Рассмотрим естественное отображение

$$\mathrm{cl} : \mathbb{Z}_B^0 \to J(C_{f,3})(\bar{K},)$$

которое переводит любой дивизор вида $\sum_{P\in B} a_P(P)$ в (его класс линейной эквивалентности, т.е., в)

$$\sum_{P\in B} a_P j(P) \in J(C_{f,3})(\bar{K}).$$

Оказывается, $\mathrm{cl}(\mathbb{Z}_B^0) = J(C_{f,3})^{\delta_3}$ и ядро гомоморфизма cl совпадает с $3 \cdot \mathbb{Z}_B^0$. Это позволяет определить естественный изоморфизм модулей Галуа $\mathbb{Z}_B^0/3\mathbb{Z}_B^0$ и $J(C_{f,3})^{\delta_3}$ и мы получаем естественный изоморфизм модулей Галуа

$$\overline{\mathrm{cl}} : V_f = \mathbb{Z}_B^0/3\mathbb{Z}_B^0 \cong J(C_{f,3})^{\delta_3}.$$

Поскольку δ_2 коммутирует с δ_3, подмодуль Галуа $J(C_{f,3})^{\delta_3}$ является δ_2-инвариантным. Из явного описания гомоморфизмов cl и D_2 вытекает, что если $\bar{\mathrm{cl}}(\phi) = P \in$

$J(C_{f,3})^{\delta_3}$ то $\delta_2 P$ - образ (при отображении $\overline{\mathrm{cl}}$) функции $\alpha \to \phi(-\alpha)$. Другими словами,

$$\overline{\mathrm{cl}}(D_2\phi) = \delta_2\overline{\mathrm{cl}}(\phi)\ \forall \phi \in V_f.$$

Отсюда вытекает, что ограничение гомоморфизма $\overline{\mathrm{cl}}$ на подмодуль V_f^- дает нам изоморфизм модулей Галуа

$$\overline{\mathrm{cl}} : V_f^- \cong \{P \in J(C_{f,3})^{\delta_3} \mid \delta_2 P = -P\}.$$

Отсюда следует, что

$$\{P \in J(C_{f,3})^{\delta_3} \mid \delta_2 P = -P\} = \overline{\mathrm{cl}}(V_f^-) = \overline{\mathrm{cl}}((1-D_2)V_f) = (1-\delta_2)J(C_{f,3})^{\delta_3}.$$

3.3. Тригональные примианы. Рассмотрим многообразие Прима

$$P(C_{f,3}) = (1-\delta_2)J(C_{f,3}) \subset J(C_{f,3}).$$

Если ограничить каноническую главную поляризацию якобиана $J(C_{f,3})$ на его абелево подмногообразие $P(C_{f,3})$, то индуцированная поляризация является главной поляризацией на $P(C_{f,3})$, умноженной на два [4, Параграф 3, Следствие 2]. Ясно, что "индуцированная"главная поляризация на $P(C_{f,3})$ является δ_3-инвариантной. Также ясно [4, Параграф 3, Следствие 2], что $P(C_{f,3})$ совпадает со связной компонентой единицы естественного сюръективного гомоморфизма якобианов $J(C_{f,3}) \to J(\tilde{C}_{f,3})$; в частности, $P(C_{f,3})$ - m-мерное абелево многообразие, определенное над K. Ясно, что абелево подмногообразие $P(C_{f,3})$ is δ_3-инвариантно. Следовательно, мы можем и будем рассматривать δ_3 как K-автоморфизм абелева многообразия $P(C_{f,3})$. По-прежнему, $\delta_3^2 + \delta_3 + 1 = 0$ в $\mathrm{End}(P(C_{f,3}))$. Как и выше, это равенство задает вложение колец

$$\mathbb{Z}[\zeta_3] \hookrightarrow \mathrm{End}(P(C_{f,3})),\ \zeta_3 \mapsto \delta_3.$$

С другой стороны, $1+\delta_2$ kills $P(C_{f,3})$, потому что

$$0 = 1 - \delta_2^2 = (1+\delta_2)(1-\delta_2) \in \mathrm{End}(J(C_{f,3}))$$

и $P(C_{f,3})(\bar{K}) = (1-\delta_2)(J(C_{f,3}))$. Отсюда вытекает, что

$$\delta_2 P = -P\ \forall P \in P(C_{f,3})(\bar{K}).$$

Рассмотрим (под)модуль Галуа $P(C_{f,3})^{\delta_3}$ всех δ_3-инвариантов в $P(C_{f,3})(\bar{K})$. Ясно, что

$$P(C_{f,3})^{\delta_3} \subset \{P \in J(C_{f,3})^{\delta_3} \mid \delta_2 P = -P\}.$$

Поскольку последняя группа совпадает с $(1-\delta_2)J(C_{f,3})^{\delta_3}$, мы заключаем, что

$$P(C_{f,3})^{\delta_3} = \{P \in J(C_{f,3})^{\delta_3} \mid \delta_2 P = -P\}.$$

Отсюда вытекает, что модули Галуа $P(C_{f,3})^{\delta_3}$ and V_f^- канонически изоморфны.

Положим

$$\mathcal{O} = \mathbb{Z}[\mu_3],\ \lambda = (1-\gamma)\mathcal{O},\ E = \mathcal{O}\otimes\mathbb{Q} = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}).$$

Тогда поле вычетов

$$\mathcal{O}/\lambda = \mathbb{F}_3.$$

Напомним, что имеется естественный гомоморфизм

$$\mathcal{O} = \mathbb{Z}[\mu_3] \hookrightarrow \mathrm{End}_K(P(C_{f,3})), \zeta_3 \mapsto \delta_3.$$

Это дает нам равенство

$$P(C_{f,3})^{\delta_3} = P(C_{f,3})_\lambda$$

и, следовательно, модули Галуа $P(C_{f,3})_\lambda$ и V_f^- канонически изоморфны. В частности,

$$\dim_{\mathbb{F}_3} P(C_{f,3})_\lambda = m.$$

С другой стороны, хорошо известно [12, 8, 19], что $P(C_{f,3})_\lambda$ - свободный $\mathcal{O}/\lambda$-модуль ранга $2\dim(P(C_{f,3}))/[E:\mathbb{Q}]$. Поскольку $\mathcal{O}/\lambda = \mathbb{F}_3$ and $[E:\mathbb{Q}] = 2$, мы получаем другое доказательство равенства $\dim(P(C_{f,3})) = m$. Заметим, что

$$\dim(P(C_{f,3})) = m = \dim_{\mathbb{F}_3}(\Omega^1(C_{f,3})^-).$$

Замечание 3.4. Принимая во внимание то, что $\dim(P(C_{f,3})) = m$ и применяя Теорему 3.10 работы [18] к

$$Y = J(C_{f,3}), Z = P(C_{f,3}), \delta = \delta_2, P(t) = 1 - t,$$

мы находим, что гомоморфизм абелевых многообразий $1 - \delta_2 : J(C_{f,3}) \twoheadrightarrow P(C_{f,3}) \subset J(C_{f,3})$ индуцирует (на дифференциалах первого рода) изоморфизм векторных пространств

$$(1 - \delta_2)^* : \Omega^1(P(C_{f,3})) \cong \Omega^1(C_{f,3})^- \subset \Omega^1(J(C_{f,3})),$$

и изоморфизм этот δ_3-эквивариантен. Отсюда легко вытекает, что δ_3 индуцирует линейный оператор в пространстве $\Omega^1(P(C_{f,3}))$, спектр которого состоит из собственных чисел γ^{-1} кратности $2k+1$ и $\gamma = \gamma^{-2}$ кратности $4k+4$. Ясно, что числа $2k+1$ and $4k+4$ *взаимно просты.*

Теорема 3.5. *Предположим, что существует дважды транзитивная группа перестановок $\mathcal{G} \subset \mathbf{S}_m$, удовлетворяющая следующим условиям:*

(i) *Группа $\mathcal{G}$ не содержит нормальную подгруппу с индексом, делящим m (за исключением себя самой).*
(ii) *Группа* $\mathrm{Gal}(h)$ *содержит* $2^{m-1} \cdot \mathcal{G}$.

Тогда $\mathrm{End}(P(C_{f,3})) = \mathbb{Z}[\zeta_3]$. *В частности, $P(C_{f,3})$ - абсолютно простое абелево многообразие.*

Доказательство. Заменяя в случае необходимости поле K на его расширение, мы можем и будем предполагать, что $\mathrm{Gal}(h) = 2^{m-1} \cdot \mathcal{G}$. Отождествляя группу $\mathrm{Perm}(\mathfrak{R}_h)$ со стабилизатором корня 0 в $\mathrm{Perm}(\mathfrak{R}_f)$, мы получаем, что

$$\mathrm{Gal}(f) = \mathrm{Gal}(h) = 2^{m-1} \cdot \mathcal{G}.$$

Поскольку модули Галуа $P(C_{f,3})_\lambda$ и V_f^- изоморфны, из Леммы 2.9 вытекает, что $\mathrm{End}_{\mathrm{Gal}(K)}(P(C_{f,3})_\lambda)^{\delta_3}) = \mathbb{F}_3$. Теперь Теорема 3.5 вытекает из Замечания 3.4 и Теоремы 3.12(ii)(2) работы [19], примененных к $X = P(C_{f,3}), E = \mathbb{Q}(\sqrt{-3}), \mathcal{O} = \mathbb{Z}[\mu_3], \lambda = (1-\gamma)\mathcal{O}$. □

Пример 3.6. Пусть $m = 6k+5$ - натуральное число, сравнимое с 5 по модулю 6. Пусть L - поле рациональных функций $\mathbb{C}(t_1, \dots, t_m)$ от m независимых переменных $t_1, \dots, t_m$ over $\mathbb{C}$. Можно реализовать группу $2^m \cdot \mathbf{S}_m$ как группу всех линейных преобразований поля L вида

$$(s; \epsilon_1, \dots, \epsilon_m) : t_i \mapsto \epsilon_i t_{s(i)},\ i = 1, \dots m$$

где

$$s \in \mathbf{S}_m,\ \epsilon_i = \pm 1.$$

Пусть K - подполе всех $2^m \cdot \mathbf{S}_m$-инвариантов в L. Ясно, что L/K - конечное расширение Галуа с группой Галуа $2^m \cdot \mathbf{S}_m$. В частности, $\bar{L} = \bar{K}$. Поскольку $m \geq$

5, список нормальных подгрупп в $\mathbf{S}_m$ исчерпывается подгруппой $\{1\}$ четного индекса $m!$, знакопеременной подгруппой $\mathbf{A}_m$ индекса 2 и самой группой $\mathbf{S}_m$.

Многочлен

$$h(x) = \prod_{i=1}^{m}(x^2 - t_i^2) = \prod_{i=1}^{m}(x - t_i)\prod_{i=1}^{m}(x + t_i)$$

четной степени $2m$ лежит в $K[x]$, а его поле разложения совпадает с L. Отсюда вытекает, что $\mathrm{Gal}(h) = 2^m \cdot \mathbf{S}_m$. Применяя Теорему 3.5 к многочлену

$$f(x) := x \cdot h(x) = x \cdot \prod_{i=1}^{m}(x^2 - t_i^2)$$

нечетной степени $(2m+1)$, мы заключаем, что кольцо эндоморфизмов (над $\bar{L}$) m-мерного примиана $P(C_{f,3})$ совпадает с $\mathbb{Z}[\zeta_3]$.

Доказательство Теоремы 1.1. Все утверждения (i) и(ii)(a) за исключением (i)(1)(C) уже доказаны в разделах 3.3 и Замечании 3.4. Поскольку $\mathbf{S}_m$ - дважды транзитивная группа перестановок, не имеющая нормальных делителей нечетного индекса (за исключением себя самой) и $\mathbb{W}(\mathbb{D}_m) = 2^{m-1} \cdot \mathbf{S}_m$, то утверждение (ii)(b1) вытекает из Теоремы 3.5, примененной к $\mathcal{G} = \mathbf{S}_m$.

Для доказательства утверждения (i)(1)(C), заметим, что

$$3 \cdot \mid (2k+1) - (4k+4) \mid = 6k + 9 > (6K + 5) + 2 = m + 2 = \dim(P(C_{f,3})) + 2.$$

Теперь утверждение (i)(1)(C)) вытекает из утверждения (i)(2), благодаря Теореме 1.1 работы [20].

Для доказательства утверждения (ii)(b2), заметим, что мы уже знаем (благодаря уже доказанному утверждению (ii)(b1)), что $\mathrm{End}(P(C_{f,3})) = \mathbb{Z}[\delta_3] \cong \mathbb{Z}[\zeta_3]$. Отсюда вытекает, что $P(C_{f,3})$ абсолютно просто и имеет ровно одну главную поляризацию, которая δ_3-инвариантна. Таким образом, если $P(C_{f,3})$ изоморфно якобиану гладкой проективной прямой, то этот изоморфизм переводит друг в друга соответствующие главные поляризации.

Теперь утверждение (ii)(b2) вытекает из утверждения (i)(1)(C).

□

Список литературы

[1] W. Bosma, J. Cannon, C. Playoust, *The Magma Algebra System I: The User Language*. J. Symb. Comp. **24** (1997), 235–265; http://magma.maths.usyd.edu.au/magma/ .

[2] J. K. Koo, *On holomorphic differentials of some algebraic function field of one variable over C*. Bull. Austral. Math. Soc. **43** (1991), 399-405.

[3] K. Matsumoto, T. Terasoma, *Theta constants associated to cubic threefolds*. J. Algebraic Geom. **12** (2003), 741–775.

[4] D. Mumford, *Prym varieties* I. In: Contributions to Analysis, pp. 325–350. Academic Press 1974.

[5] Oort, F. *Endomorphism algebras of abelian varieties*. In: Algebraic geometry and commutative algebra, Vol. II, 469–502, Kinokuniya, Tokyo, 1988.

[6] D.S. Passman, Permutation groups. W.A. Benjamin, Inc., New York and Amsterdam, 1968.

[7] B. Poonen, E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*. J. reine angew. Math. **488** (1997), 141-188.

[8] Ribet, K.: Galois action on division points of Abelian varieties with real multiplications. Amer. J. Math. **98**, 751–804 (1976)

[9] E. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*. Math. Ann. **310** (1998), 447–471; Erratum, Math. Ann. **339** (2007), 1.

[10] J.-P. Serre, Topics in Galois Theory. Jones and Bartlett Publishers, Boston-London (1992).

[11] Shimura, G. *On analytic families of polarized abelian varieties and automorphic functions.* Ann. of Math. (2) 78 1963 149–192.
[12] Shimura, G., Introduction to the arithmetic theory of automorphic functions. Princeton University Press, Princeton (1971).
[13] Shokurov, V. V., *Distinguishing Prymians from Jacobians.* Invent. Math. **65** (1981/82), no. 2, 209–219.
[14] Шокуров В.В., Многообразия Прима: теория и приложения. Известия АН СССР сер. матем. **47** (1983), no. 4, 785–855; Math. USSR-Izv. **23** (1984), no. 1, 83–147.
[15] C. Towse, *Weierstrass points on cyclic covers of the projective line.* Trans. AMS **348** (1996), 3355-3377.
[16] Yu. G. Zarhin, *Cyclic covers, their jacobians and endomorphisms.* J. reine angew. Math. **544** (2002), 91–110.
[17] Yu. G. Zarhin, *The endomorphism rings of jacobians of cyclic covers of the projective line.* Math. Proc. Cambridge Philos. Soc. **136** (2004), 257–267.
[18] Yu. G. Zarhin, *Endomorphism algebras of superelliptic Jacobians.* In: Geometric methods in algebra and number theory (F. Bogomolov, Yu. Tschinkel, eds), 339–362, Progr. Math., 235, Birkhäuser Boston, Boston, MA, 2005.
[19] Yu. G. Zarhin, *Endomorphisms of superelliptic jacobians.* Math. Z., DOI: 10.1007/s00209-008-0342-5; Erratum, DOI: 10.1007/s00209-008-0377-7 .
[20] Yu. G. Zarhin, *Cubic surfaces and cubic threefolds, jacobians and intermediate jacobians.* In: Algebra, Arithmetic and Geometry (Manin Festschrift), Progress in Math., Birkhäuser, 2008, to appear; arXiv:math/0610138v3 [math.AG] .

Pennsylvania State University, Department of Mathematics, University Park, PA 16802, USA

Институт Математических Проблем Биологии РАН, Московская обл., г. Пущино

E-mail address: zarhin@math.psu.edu