Ю. Г. Зархин, Гомоморфизмы гиперэллиптических якобианов, *Труды МИАН*, 2003, том 241, 90–104

ТРУДЫ МАТЕМАТИЧЕСКОГО ИНСТИТУТА ИМ. В.А. СТЕКЛОВА, 2003, т. 241, с. 90–104

УДК 512.7

Гомоморфизмы гиперэллиптических якобианов[1]

©2003 г. Ю. Г. Зархин[2]

Поступило в декабре 2002 г.

Пусть K — поле характеристики, отличной от 2, и K_a — его алгебраическое замыкание. Пусть $n \geq 5$ и $m \geq 5$ — натуральные числа. Пусть $f(x), h(x) \in K[x]$ — неприводимые сепарабельные многочлены степени n и m соответственно. Предположим дополнительно, что $n \geq 9$, если характеристика поля K положительна. Предположим, что группа Галуа многочлена f совпадает либо с полной симметрической группой $\mathbf{S}_n$, либо с знакопеременной группой $\mathbf{A}_n$, а группа Галуа многочлена h совпадает либо с полной симметрической группой $\mathbf{S}_m$, либо с знакопеременной группой $\mathbf{A}_m$. Рассмотрим гиперэллиптические кривые $C_f\colon y^2 = f(x)$ и $C_h\colon y^2 = h(x)$. Пусть $J(C_f)$ и $J(C_h)$ — якобианы кривых C_f и C_h соответственно. Ранее автор доказал, что $J(C_f)$ — абсолютно простое абелево многообразие без нетривиальных эндоморфизмов над K_a. В настоящей работе мы доказываем, что абелевы многообразия $J(C_f)$ и $J(C_h)$ неизогенны над K_a, если поля разложения многочленов f и h линейно разделены над K.

1. ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ, ФОРМУЛИРОВКИ

Пусть K — поле. Зафиксируем алгебраическое замыкание K_a поля K и обозначим через $\mathrm{Gal}(K)$ его абсолютную группу Галуа $\mathrm{Aut}(K_a/K)$. Если X — абелево многообразие над K_a, то мы обозначаем через $\mathrm{End}(X)$ кольцо всех его K_a-эндоморфизмов. Если Y — (возможно, другое) абелево многообразие над K_a, то мы обозначаем через $\mathrm{Hom}(X,Y)$ группу всех K_a-гомоморфизмов из X в Y. Хорошо известно, что $\mathrm{Hom}(X,Y) = 0$ тогда и только тогда, когда $\mathrm{Hom}(Y,X) = 0$. Легко видеть, что если $\mathrm{End}(X) = \mathbb{Z}$ и $\dim(X) \geq \dim(Y)$, то $\mathrm{Hom}(X,Y) = 0$ тогда и только тогда, когда X и Y *неизогенны* над K_a.

Пусть $f(x) \in K[x]$ — многочлен степени $n \geq 3$ без кратных корней. Обозначим через $\mathfrak{R}_f \subset K_a$ множество корней многочлена f, через $K(\mathfrak{R}_f) \subset K_a$ его поле разложения, а через $\mathrm{Gal}(f) = \mathrm{Aut}(K(\mathfrak{R}_f)/K) = \mathrm{Gal}(K(\mathfrak{R}_f)/K)$ группу Галуа многочлена f. Хорошо известно, что множество $\mathfrak{R}_f$ состоит из $n = \deg(f)$ элементов. Группа $\mathrm{Gal}(f)$ переставляет элементы $\mathfrak{R}_f$ и тем самым отождествляется с некоторой подгруппой группы $\mathrm{Perm}(\mathfrak{R}_f)$ всех перестановок множества $\mathfrak{R}_f$. Ясно, что любое упорядочение множества $\mathfrak{R}_f$ задает изоморфизм между $\mathrm{Perm}(\mathfrak{R}_f)$ и полной симметрической группой $\mathbf{S}_n$, превращая $\mathrm{Gal}(f)$ в некоторую подгруппу группы $\mathbf{S}_n$. (Хорошо известно, что эта подгруппа перестановок транзитивна тогда и только тогда, когда многочлен f неприводим.)

Предположим, что $\mathrm{char}(K) \neq 2$, и рассмотрим гиперэллиптическую кривую

$$C_f\colon\ y^2 = f(x),$$

определенную над K. Ее род $g = g(C_f)$ равен $(n-1)/2$, если n нечетно, и $(n-2)/2$, если n четно. Пусть $J(C_f)$ — якобиан кривой C_f; это g-мерное абелево многообразие над K_a, определенное над K.

В работах автора [20, 22, 23] доказано следующее утверждение.

[1]Работа выполнена при финансовой поддержке Национального научного фонда США (NSF).

[2]Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA;
Институт математических проблем биологии РАН, Пущино, Московская область, Россия.
E-mail: zarhin@math.psu.edu

Теорема 1.1. *Пусть K — поле характеристики, отличной от 2. Пусть $n \ge 5$ — натуральное число. Предположим, что $f(x) \in K[x]$ — неприводимый многочлен степени $n \ge 5$. Предположим также, что если $\mathrm{char}(K) > 0$, то $n \ge 9$, а многочлен $f(x)$ не имеет кратных корней. Пусть группа Галуа многочлена $f(x)$ совпадает либо с полной симметрической группой $\mathbf{S}_n$, либо с знакопеременной группой $\mathbf{A}_n$.*

Тогда $\mathrm{End}(J(C_f)) = \mathbb{Z}$.

Основной результат настоящей работы — следующее утверждение.

Теорема 1.2 (основная теорема)**.** *Пусть K — поле характеристики, отличной от 2, а K_a — его алгебраическое замыкание. Пусть $f(x), h(x) \in K[x]$ — неприводимые многочлены степени $n \ge 3$ и $m \ge 3$ соответственно. Пусть поля разложения многочленов f и h линейно разделены над K. Предположим также, что если $\mathrm{char}(K) > 0$, то $n = \deg(f) \ge 9$, а многочлены $f(x)$ и $h(x)$ не имеют кратных корней.*

Пусть выполнены следующие условия:

(i) $\mathrm{Gal}(h) = \mathbf{A}_m$ *или* $\mathbf{S}_m$;

(ii) *либо* $\mathrm{Gal}(f) = \mathbf{S}_n$, *либо* $\mathrm{Gal}(f) = \mathbf{A}_n$, $n \ge 5$.

Тогда

$$\mathrm{Hom}(J(C_f), J(C_h)) = 0, \qquad \mathrm{Hom}(J(C_h), J(C_f)) = 0.$$

Мы докажем теорему 1.2 в разд. 2.

Пример 1.3. Пусть $n \ge 3$ — натуральное число. Хорошо известно [16, p. 139], что группа Галуа многочлена $x^n - x - t$ над полем рациональных функций $\mathbb{Q}(t)$ совпадает с полной симметрической группой $\mathbf{S}_n$. Из теоремы Гильберта о неприводимости вытекает существование *бесконечного* множества рациональных чисел $S \subset \mathbb{Q}$ такого, что для каждого $r \in S$ группа Галуа $\mathrm{Gal}(u_r)$ многочлена

$$u_r(x) = x^n - x - r \in \mathbb{Q}[x]$$

совпадает с $\mathbf{S}_n$, а для *различных* $r, k \in S$ поля разложения многочленов u_r и u_k линейно разделены над $\mathbb{Q}$. Рассмотрим якобианы $J(C_{u_r})$ и $J(C_{u_k})$ гиперэллиптических кривых $C_{u_r}\colon y^2 = u_r(x)$ и $C_{u_k}\colon y^2 = u_k(x)$, определенные над $\mathbb{Q}$. Отметим, что если $n < 5$, то $J(C_{u_r})$ и $J(C_{u_k})$ — эллиптические кривые. Применяя теоремы 1.2 и 1.1 к многочленам u_r и u_k, мы получаем, что для всех $n \ge 3$ якобианы $J(C_{u_r})$ и $J(C_{u_k})$ абсолютно просты и попарно неизогенны над $\overline{\mathbb{Q}}$ (и, следовательно, над $\mathbb{C}$). В частности, для любого натурального числа g множество классов изогений абсолютно простых g-мерных абелевых многообразий над $\mathbb{Q}$ бесконечно. (Для эллиптических кривых это утверждение хорошо известно.) Также из теоремы 1.1 вытекает, что для любого натурального числа $g > 1$ множество классов изогений абсолютно простых g-мерных абелевых многообразий над $\mathbb{Q}$ без нетривиальных эндоморфизмов над $\mathbb{C}$ является бесконечным. (Аналогичное утверждение для эллиптических кривых также хорошо известно: достаточно рассмотреть для каждого простого p эллиптическую кривую с j-инвариантом $1/p$.)

Следствие 1.4. *Пусть K — поле характеристики, отличной от 2, а K_a — его алгебраическое замыкание. Пусть $f(x), h(x) \in K[x]$ — неприводимые многочлены степени $n \ge 5$ и $m \ge 3$ соответственно. Предположим также, что если $\mathrm{char}(K) > 0$, то $n = \deg(f) \ge 9$, а оба многочлена $f(x)$ и $h(x)$ не имеют кратных корней. Пусть выполнены следующие условия*:

(i) $\mathrm{Gal}(h) = \mathbf{A}_m$ *или* $\mathbf{S}_m$;

(ii) $\mathrm{Gal}(f) = \mathbf{S}_n$ *или* $\mathrm{Gal}(f) = \mathbf{A}_n$;

(iii) *либо* $n \ne m$, *либо* $\mathrm{Gal}(f) = \mathbf{S}_n$ *и* $\mathrm{Gal}(h) = \mathbf{A}_m$.

Тогда

$$\mathrm{Hom}(J(C_f), J(C_h)) = 0, \qquad \mathrm{Hom}(J(C_h), J(C_f)) = 0.$$

Следствие 1.5. *Пусть K — поле характеристики, отличной от 2, а K_a — его алгебраическое замыкание. Пусть $n \geq 5$ — натуральное число, не равное 6. Пусть $f(x), h(x) \in K[x]$ — неприводимые многочлены одной и той же степени n. Предположим также, что если $\mathrm{char}(K) > 0$, то $n \geq 9$, а оба многочлена $f(x)$ и $h(x)$ не имеют кратных корней. Пусть выполнены следующие условия*:

(i) $\mathrm{Gal}(h) = \mathbf{A}_n$ *или* $\mathbf{S}_n$;

(ii) $\mathrm{Gal}(f) = \mathbf{S}_n$ *или* $\mathrm{Gal}(f) = \mathbf{A}_n$;

(iii) *если* $K_f := K[x]/fK[x]$, $K_h := K[x]/hK[x]$, *то расширения полей* K_f/K *и* K_h/K *неизоморфны.*

Тогда

$$\mathrm{Hom}(J(C_f), J(C_h)) = 0, \qquad \mathrm{Hom}(J(C_h), J(C_f)) = 0.$$

Мы докажем следствия 1.4 и 1.5 в разд. 4.

2. ДОКАЗАТЕЛЬСТВО ОСНОВНОЙ ТЕОРЕМЫ

Пусть d — натуральное число, не делящееся на характеристику поля K. Пусть X — абелево многообразие положительной размерности, определенное над K. Обозначим через X_d ядро умножения на d в $X(K_a)$. Известно [14], что коммутативная группа X_d — свободный $\mathbb{Z}/d\mathbb{Z}$-модуль ранга $2\dim(X)$. Легко видеть, что X_d — подмодуль Галуа в $X(K_a)$. Обозначим через

$$\widetilde{\rho}_{d,X}\colon\ \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Z}/d\mathbb{Z}}(X_d) \cong \mathrm{GL}(2\dim(X), \mathbb{Z}/d\mathbb{Z})$$

соответствующий (непрерывный) гомоморфизм, задающий действие группы Галуа на X_d. Положим

$$\widetilde{G}_{d,X} = \widetilde{\rho}_{d,X}(\mathrm{Gal}(K)) \subset \mathrm{Aut}_{\mathbb{Z}/d\mathbb{Z}}(X_d).$$

Ясно, что $\widetilde{G}_{d,X}$ совпадает с группой Галуа расширения $K(X_d)/K$, где $K(X_d)$ — поле определения всех точек на X, порядок которых делит d. В частности, если ℓ — простое число $\neq \mathrm{char}(K)$, то X_ℓ — векторное пространство над простым полем $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$ размерности $2\dim(X)$ и включение $\widetilde{G}_{\ell,X} \subset \mathrm{Aut}_{\mathbb{F}_\ell}(X_\ell)$ задает точное линейное представление группы $\widetilde{G}_{\ell,X}$ в векторном пространстве X_ℓ. Мы выведем теорему 1.2 из следующего вспомогательного утверждения, представляющего некоторый самостоятельный интерес.

Теорема 2.1. *Пусть ℓ — простое число, K — поле характеристики, отличной от ℓ, X и Y — абелевы многообразия положительной размерности, определенные над K. Предположим, что выполнены следующие условия*:

(i) *расширения $K(X_\ell)$ и $K(Y_\ell)$ линейно разделены над K*;

(ii) *естественное представление группы $\widetilde{G}_{\ell,X}$ в пространстве X_ℓ абсолютно неприводимо*;

(iii) *естественное представление группы $\widetilde{G}_{\ell,Y}$ в пространстве Y_ℓ неприводимо.*

Тогда либо

$$\mathrm{Hom}(X, Y) = 0, \qquad \mathrm{Hom}(Y, X) = 0,$$

либо $\mathrm{char}(K) > 0$ *и оба абелевых многообразия X и Y суперсингулярны.*

Мы докажем теорему 2.1 в разд. 3.

На самом деле мы будем доказывать не теорему 1.2, а некоторое ее обобщение. Чтобы сформулировать это обобщение, нам понадобится ввести определения *хороших* и *очень хороших* многочленов. Но вначале напомним некоторые стандартные обозначения [3, §2.8]. Так, $\mathbb{F}_q$ обозначает конечное поле характеристики p, состоящее из q элементов, $\mathrm{GL}(d,q) := \mathrm{GL}(d,\mathbb{F}_q)$ — группа обратимых линейных преобразований d-мерного векторного пространства $\mathbb{F}_q^d$, $\mathrm{SL}(d,q) := \mathrm{SL}(d,\mathbb{F}_q)$ — ее подгруппа, состоящая из всех матриц с определителем 1, а $\mathrm{PGL}(d,q) = \mathrm{PGL}(d,\mathbb{F}_q)$ и $\mathbf{L}_d(q) = \mathrm{PSL}(d,q) = \mathrm{PSL}(d,\mathbb{F}_q)$ — соответствующие фактор-группы по подгруппе всех скаляров, рассматриваемые как группы преобразований проективного пространства $\mathbf{P}^{d-1}(\mathbb{F}_q)$. Кроме того, $\mathrm{AGL}(d,q) := \mathrm{AGL}(d,\mathbb{F}_q)$ — группа всех аффинных преобразований пространства $\mathbb{F}_q^d$, являющаяся полупрямым произведением группы $\mathrm{GL}(d,q)$ и группы $\mathbb{F}_q^d$ всех параллельных переносов. Обозначим через $\mathrm{Fr}\colon \mathbb{F}_q^d \to \mathbb{F}_q^d$ автоморфизм Фробениуса

$$(a_1,\dots,a_d) \mapsto (a_1^p,\dots,a_d^p).$$

Через $\Gamma\mathbf{L}(d,q)$, $\Sigma\mathbf{L}(d,q)$ и $\mathbf{A}\Sigma\mathbf{L}(d,q)$ обозначаются группы преобразований пространства $\mathbb{F}_q^d$, порожденные Fr и подгруппами $\mathrm{GL}(d,q)$, $\mathrm{SL}(d,q)$ и $\mathrm{AGL}(d,q)$ соответственно. Через $\mathbf{P}\Gamma\mathbf{L}(d,q)$ и $\mathbf{P}\Sigma\mathbf{L}(d,q)$ обозначаются группы преобразований проективного пространства $\mathbf{P}^{d-1}(\mathbb{F}_q)$, индуцированные (являющиеся фактор-группами по подгруппам всех скаляров) группами $\Gamma\mathbf{L}(d,q)$ и $\Sigma\mathbf{L}(d,q)$ соответственно.

Пусть $f(x) \in K[x]$ — сепарабельный неприводимый многочлен степени $n \geq 3$. Будем говорить, что f *очень хорош*, если выполнено одно из следующих условий.

(s) $\mathrm{Gal}(f) = \mathbf{S}_n$.

(a) $\mathrm{Gal}(f) = \mathbf{A}_n$ и $n \geq 5$.

(m) $n = 11$ или 12 и $\mathrm{Gal}(f)$ — соответствующая маленькая группа Матье M_n, четырежды (или пятикратно) транзитивно действующая на $\mathfrak{R}_f$.

(l11) $n = 11$ и $\mathrm{Gal}(f) = \mathbf{L}_2(11) = \mathrm{PSL}_2(\mathbb{F}_{11})$ дважды транзитивно действует на $\mathfrak{R}_f$.

(m12) $n = 12$ и $\mathrm{Gal}(f) = \mathrm{M}_{11}$ трижды транзитивно действует на $\mathfrak{R}_f$.

(aff) Существуют нечетное простое число p, его целая положительная степень q и натуральное число d такие, что $n = p^d > 3$ и можно отождествить $\mathfrak{R}_f$ с $\mathbb{F}_q^d$ таким образом, что $\mathrm{Gal}(f)$ превращается в *дважды* или *трижды транзитивную* подгруппу группы $\mathrm{AGL}(d,q)$, содержащую группу $\mathbb{F}_q^d$ всех параллельных переносов.

(p) Существуют нечетное простое число p, его целая положительная степень q и натуральное число $d \geq 3$ такие, что $n = \frac{q^d-1}{q-1}$ и можно отождествить $\mathfrak{R}_f$ с $\mathbf{P}^{d-1}(\mathbb{F}_q)$ таким образом, что $\mathrm{Gal}(f)$ становится подгруппой группы $\mathbf{P}\Gamma\mathbf{L}(d,q)$, содержащей $\mathrm{PSL}(d,q)$.

(p1) Существуют нечетное простое число p и его целая положительная степень q такие, что $n = q+1$ и можно отождествить $\mathfrak{R}_f$ с проективной прямой $\mathbf{P}^1(\mathbb{F}_q)$ таким образом, что $\mathrm{Gal}(f)$ становится трижды транзитивной подгруппой группы $\mathbf{P}\Gamma\mathbf{L}(2,q)$.

(p2) Существует натуральное число $d \geq 2$ такое, что $q := 2^d$, $n = q+1$ и можно отождествить $\mathfrak{R}_f$ с проективной прямой $\mathbf{P}^1(\mathbb{F}_q)$ таким образом, что $\mathrm{Gal}(f)$ становится подгруппой группы $\mathbf{P}\Gamma\mathbf{L}(d,q)$, содержащей $\mathrm{PSL}(2,q)$.

(u3) Существует натуральное число $d \geq 2$ такое, что $q := 2^d$, $n = q^3+1$ и можно отождествить $\mathfrak{R}_f$ с множеством изотропных прямых (эрмитовой кривой) в $\mathbb{F}_{q^2}^3$ относительно некоторой невырожденной эрмитовой формы таким образом, что $\mathrm{Gal}(f)$ становится группой, содержащей проективную специальную унитарную группу $\mathrm{U}_3(q) := \mathrm{PSU}(3,q) = \mathrm{PSU}(3,\mathbb{F}_{q^2})$, дважды транзитивно действующую на $\mathfrak{R}_f$.

(sz) Существует натуральное число d такое, что $q := 2^{2d+1}$, $n = q^2+1$, а $\mathrm{Gal}(f)$ содержит подгруппу, изоморфную группе Судзуки $\mathrm{Sz}(q)$, дважды транзитивно действующей на $\mathfrak{R}_f$.

Многочлен f называется *хорошим*, если либо он очень хороший, либо выполнено одно из следующих условий.

(a3) $n = 3$ и $\mathrm{Gal}(f) = \mathbf{A}_3$.

(a4) $n = 4$ и $\mathrm{Gal}(f) = \mathbf{A}_4$.

(p3) Существуют нечетное простое число p и его целая положительная степень q такие, что $n = q + 1$ и можно отождествить $\mathfrak{R}_f$ с проективной прямой $\mathbf{P}^1(\mathbb{F}_q)$ таким образом, что $\mathrm{Gal}(f)$ становится дважды транзитивной подгруппой группы $\mathbf{P\Gamma L}(2, q)$. При этом q должно быть сравнимо либо с 3, либо с 5 по модулю 8.

Замечание 2.2. Дважды транзитивное действие групп Судзуки $\mathrm{Sz}(q)$ (случай (sz)) явно описано на с. 184–187 книги [5]; о связях с гиперэллиптическими якобианами см. [21]. По поводу дважды транзитивного действия проективной специальной унитарной группы U_3 на эрмитову кривую (случай (u3)) см. [4, Kap. II, Satz 4.12; 3, p. 248–250]; о связях с гиперэллиптическими якобианами см. [24].

Чтобы объяснить, что хорошего в хороших полиномах, напомним определение *сердечника* (heart) группы $\mathrm{Gal}(f)$, действующей на множестве $\mathfrak{R}_f$ [12, 21].

Пусть $\mathfrak{R} = \mathfrak{R}_f = \{a_1, \dots, a_n\} \subset K_a$ — множество всех корней многочлена f. Мы можем рассматривать группу $\mathbf{S}_n$ как группу всех перестановок множества $\mathfrak{R}$. Группа Галуа $G = \mathrm{Gal}(f)$ многочлена f переставляет эти корни и тем самым реализуется как подгруппа в $\mathbf{S}_n$. Действие группы G на множестве $\mathfrak{R}$ задает стандартное *перестановочное* представление в n-мерном $\mathbb{F}_2$-векторном пространстве $\mathbb{F}_2^{\mathfrak{R}}$ всех функций $\psi\colon R \to \mathbb{F}_2$. Это представление не является неприводимым. Действительно, "прямая" постоянных функций $\mathbb{F}_2 \cdot 1$ и гиперплоскость $(\mathbb{F}_2^{\mathfrak{R}})^0 := \{\psi \mid \sum_{i=1}^n \psi(a_i) = 0\}$ являются G-инвариантными подпространствами в $\mathbb{F}_2^{\mathfrak{R}}$. Если n нечетно, то мы называем $(\mathbb{F}_2^{\mathfrak{R}})^0$ *сердечником* перестановочного действия группы $G = \mathrm{Gal}(f)$ на множество $\mathfrak{R} = \mathfrak{R}_f$ над $\mathbb{F}_2$ и обозначаем через $Q_{\mathfrak{R}} = Q_{\mathfrak{R}_f}$. Если n четно, то гиперплоскость $(\mathbb{F}_2^{\mathfrak{R}})^0$ содержит прямую $\mathbb{F}_2 \cdot 1$ и мы получаем естественное представление группы $G = \mathrm{Gal}(f)$ в $(n-2)$-мерном $\mathbb{F}_2$-векторном фактор-пространстве

$$(\mathbb{F}_2^{\mathfrak{R}})^{00} := (\mathbb{F}_2^{\mathfrak{R}})^0/(\mathbb{F}_2 \cdot 1),$$

также называемом *сердечником* перестановочного действия группы $G = \mathrm{Gal}(f)$ на множество $\mathfrak{R} = \mathfrak{R}_f$ над $\mathbb{F}_2$, и также обозначаем его через $Q_{\mathfrak{R}} = Q_{\mathfrak{R}_f}$.

Известно [7], что если n нечетно и $\mathrm{Gal}(f)$-модуль $Q_{\mathfrak{R}_f}$ абсолютно прост, то группа $\mathrm{Gal}(f)$ действует на множество $\mathfrak{R}_f$ дважды транзитивно.

Замечание 2.3. Если многочлен $f(x)$ хорош, то

(i) либо $n = 3$, $\mathrm{Gal}(f) = \mathbf{A}_3$, либо $\mathrm{Gal}(f)$ действует дважды транзитивно на $\mathfrak{R}_f$;

(ii) $\mathrm{Gal}(f)$-модуль $Q_{\mathfrak{R}_f}$ прост. При этом модуль $Q_{\mathfrak{R}_f}$ абсолютно прост, если и только если $f(x)$ *очень* хорош. Это утверждение немедленно вытекает из результатов [12, 9], за исключением легко проверяемого случая $n = 3$, $\mathrm{Gal}(f) = \mathbf{A}_3$. (См. также [21, 24].)

Замечание 2.4. Предположим, что группа перестановок $\mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f)$ изоморфна одной из *известных дважды транзитивных* групп перестановок [3, §7.7]. Тогда многочлен $f(x)$ хорош, если и только если $\mathrm{Gal}(f)$-модуль $Q_{\mathfrak{R}_f}$ прост. Это утверждение легко вытекает из результатов работ [12, 9].

Теперь мы готовы сформулировать обещанное обобщение основной теоремы.

Теорема 2.5. *Пусть K — поле характеристики, отличной от 2, а K_a — его алгебраическое замыкание. Пусть $f(x), h(x) \in K[x]$ — неприводимые многочлены без кратных корней степени $n \geq 3$ и $m \geq 3$ соответственно. Пусть поля разложения многочленов f и h линейно разделены над K. Предположим, что многочлен $f(x)$ очень хорош, а многочлен $h(x)$ хорош.*

Тогда либо

$$\operatorname{Hom}(J(C_f), J(C_h)) = 0, \qquad \operatorname{Hom}(J(C_h), J(C_f)) = 0,$$

либо $\operatorname{char}(K) > 0$ *и оба якобиана* $J(C_f)$ *и* $J(C_h)$ *— суперсингулярные абелевы многообразия.*

Доказательство. Каноническая сюръекция $\operatorname{Gal}(K) \twoheadrightarrow \operatorname{Gal}(f)$ задает на $\operatorname{Gal}(f)$-модуле $Q_{\mathfrak{R}_f}$ естественную структуру $\operatorname{Gal}(K)$-модуля. Хорошо известно, что $\operatorname{Gal}(K)$-модули $Q_{\mathfrak{R}_f}$ и $J(C_f)_2$ канонически изоморфны (см., например, [13, 11] или [21]). Отсюда, в частности, вытекает ввиду замечания 2.3, что $\widetilde{G}_{2,J(C_f)}$-модуль абсолютно прост. Аналогично каноническая сюръекция $\operatorname{Gal}(K) \twoheadrightarrow \operatorname{Gal}(h)$ задает на $\operatorname{Gal}(h)$-модуле $Q_{\mathfrak{R}_h}$ естественную структуру $\operatorname{Gal}(K)$-модуля и $\operatorname{Gal}(K)$-модули $Q_{\mathfrak{R}_h}$ и $J(C_h)_2$ канонически изоморфны. Теперь из замечания 2.3 вытекает, что $\widetilde{G}_{2,J(C_h)}$-модуль прост. Тем самым

$$K(J(C_f)_2) \subset K(\mathfrak{R}_f), \qquad K(J(C_h)_2) \subset K(\mathfrak{R}_h).$$

Поскольку расширения $K(\mathfrak{R}_f)/K$ и $K(\mathfrak{R}_h)/K$ линейно разделены, их подрасширения $K(J(C_f)_2)/K$ и $K(J(C_h)_2)/K$ также линейно разделены. Остается применить теорему 2.1 к $\ell = 2$, $X = J(C_f)$, $Y = J(C_h)$. $\square$

Замечание 2.6. На самом деле если $n \neq 4$ (соответственно $m \neq 4$), то $\operatorname{Gal}(f)$-модуль $Q_{\mathfrak{R}_f}$ точен и $K(J(C_f)_2) = K(\mathfrak{R}_f)$ (соответственно $\operatorname{Gal}(h)$-модуль $Q_{\mathfrak{R}_h}$ точен и $K(J(C_h)_2) = K(\mathfrak{R}_h)$).

Доказательство теоремы 1.2. Из теоремы 2.5 вытекает, что если существует ненулевой гомоморфизм между $J(C_f)$ и $J(C_h)$, то $\operatorname{char}(K) > 0$ и оба якобиана суперсингулярны. Однако если $\operatorname{char}(K) > 0$, то $n \geq 9$ и согласно теореме 1.1 $\operatorname{End}(J(C_f)) = \mathbb{Z}$ и, следовательно, якобиан $J(C_f)$ несуперсингулярен. $\square$

3. ГОМОМОРФИЗМЫ АБЕЛЕВЫХ МНОГООБРАЗИЙ

Для доказательства теоремы 2.1 нам понадобится следующее элементарное утверждение, хорошо известное над алгебраически замкнутыми полями в характеристике 0 [18, §3.2] (см. также теорему 10.38 из книги [2]).

Лемма 3.1. *Пусть* F *— поле,* H_1 *и* H_2 *— группы. Пусть* $\tau_1 \colon H_1 \to \operatorname{Aut}_F(W_1)$ *— неприводимое конечномерное линейное представление группы* H_1 *над* F*, а* $\tau_2 \colon H_2 \to \operatorname{Aut}_F(W_2)$ *— абсолютно неприводимое конечномерное линейное представление группы* H_2 *над* F*. Тогда естественное линейное представление*

$$\tau_1^* \otimes \tau_2 \colon\ H_1 \times H_2 \to \operatorname{Aut}_F(\operatorname{Hom}_F(W_1, W_2))$$

группы $H_1 \times H_2$ *в пространстве* $\operatorname{Hom}_F(W_1, W_2)$ *неприводимо.*

Замечание 3.2. Ясно, что представления группы $H_1 \times H_2$ в пространствах $\operatorname{Hom}_F(W_1, W_2)$ и $\operatorname{Hom}_F(W_2, W_1)$ двойственны друг другу. Поэтому из неприводимости $\operatorname{Hom}_F(W_1, W_2)$ вытекает неприводимость $\operatorname{Hom}_F(W_2, W_1)$.

Мы докажем лемму 3.1 в конце этого раздела.

Доказательство теоремы 2.1. Во-первых, заметим, что естественное представление

$$\operatorname{Gal}(K) \to \operatorname{Aut}_{\mathbb{F}_\ell}(\operatorname{Hom}_{\mathbb{F}_\ell}(Y_\ell, X_\ell))$$

неприводимо. Действительно, обозначим это представление через τ и положим

$$F = \mathbb{F}_\ell, \qquad H_1 = \widetilde{G}_{\ell,Y}, \qquad W_1 = Y_\ell, \qquad H_2 = \widetilde{G}_{\ell,X}, \qquad W_2 = X_\ell.$$

Обозначим через

$$\tau_1\colon\ H_1 = \widetilde{G}_{\ell,Y} \subset \mathrm{Aut}_{\mathbb{F}_\ell}(Y_\ell) = \mathrm{Aut}_{\mathbb{F}_\ell}(W_1)$$

и

$$\tau_2\colon\ H_2 = \widetilde{G}_{\ell,X} \subset \mathrm{Aut}_{\mathbb{F}_\ell}(X_\ell) = \mathrm{Aut}_{\mathbb{F}_\ell}(W_2)$$

соответствующие отображения включения.

Из леммы 3.1 вытекает, что линейное представление

$$\tau_1^* \otimes \tau_2\colon\ \mathrm{Gal}(K(Y_\ell)/K) \times \mathrm{Gal}(K(X_\ell)/K) \to \mathrm{Aut}_{\mathbb{F}_\ell}(\mathrm{Hom}_{\mathbb{F}_\ell}(Y_\ell, X_\ell))$$

неприводимо.

Легко видеть, что гомоморфизм τ, задающий интересующую нас структуру $\mathrm{Gal}(K)$-модуля на $\mathrm{Hom}_{\mathbb{F}_\ell}(Y_\ell, X_\ell)$, является композицией естественной сюръекции $\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(K(X_\ell, Y_\ell)/K)$, естественного вложения

$$\mathrm{Gal}(K(X_\ell, Y_\ell)/K) \hookrightarrow \mathrm{Gal}(K(Y_\ell)/K) \times \mathrm{Gal}(K(X_\ell)/K)$$

и гомоморфизма

$$\tau_1^* \otimes \tau_2\colon\ \mathrm{Gal}(K(Y_\ell)/K) \times \mathrm{Gal}(K(X_\ell)/K) \to \mathrm{Aut}_{\mathbb{F}_\ell}(\mathrm{Hom}_{\mathbb{F}_\ell}(Y_\ell, X_\ell)).$$

Здесь $K(X_\ell, Y_\ell)$ — композит полей $K(X_\ell)$ и $K(Y_\ell)$. Линейная разделенность полей $K(X_\ell)$ и $K(Y_\ell)$ означает, что

$$\mathrm{Gal}(K(X_\ell, Y_\ell)/K) = \mathrm{Gal}(K(Y_\ell)/K) \times \mathrm{Gal}(K(X_\ell)/K).$$

Отсюда вытекает, что τ является композицией *сюръективного* гомоморфизма $\mathrm{Gal}(K) \twoheadrightarrow$ $\twoheadrightarrow \mathrm{Gal}(K(Y_\ell)/K) \times \mathrm{Gal}(K(X_\ell)/K)$ и гомоморфизма $\tau_1^* \otimes \tau_2$. Поскольку представление

$$\tau_1^* \otimes \tau_2\colon\ \mathrm{Gal}(K(Y_\ell)/K) \times \mathrm{Gal}(K(X_\ell)/K) \to \mathrm{Aut}_{\mathbb{F}_\ell}(\mathrm{Hom}_{\mathbb{F}_\ell}(Y_\ell, X_\ell))$$

неприводимо, представление

$$\tau\colon\ \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{F}_\ell}(\mathrm{Hom}_{\mathbb{F}_\ell}(Y_\ell, X_\ell))$$

также неприводимо.

Во-вторых, пусть $T_\ell(X)$ и $T_\ell(Y)$ — $\mathbb{Z}_\ell$-модули Тэйта абелевых многообразий X и Y соответственно [14]. Напомним, что $T_\ell(X)$ и $T_\ell(Y)$ — свободные $\mathbb{Z}_\ell$-модули ранга $2\dim(X)$ и $2\dim(Y)$ соответственно. Также определены естественные непрерывные гомоморфизмы

$$\rho_{\ell,X}\colon\ \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(X)), \qquad \rho_{\ell,Y}\colon\ \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(Y)).$$

Имеют место естественные изоморфизмы

$$X_\ell = T_\ell(X)/\ell T_\ell(X), \qquad Y_\ell = T_\ell(Y)/\ell T_\ell(Y),$$

являющиеся изоморфизмами модулей Галуа, так что можно считать, что гомоморфизм $\widetilde{\rho}_{\ell,X}$ совпадает с редукцией гомоморфизма $\rho_{\ell,X}$ по модулю ℓ, а $\widetilde{\rho}_{\ell,Y}$ — с редукцией гомоморфизма $\rho_{\ell,Y}$. Также удобно рассматривать $\mathbb{Q}_\ell$-модули Тэйта $V_\ell(X) = T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ и $V_\ell(Y) =$ $= T_\ell(Y) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ — векторные пространства над полем $\mathbb{Q}_\ell$ размерности $2\dim(X)$ и $2\dim(Y)$

соответственно. Группы $T_\ell(X)$ и $T_\ell(Y)$ естественно отождествляются с $\mathbb{Z}_\ell$-решетками в $V_\ell(X)$ и $V_\ell(Y)$ соответственно, и включения

$$\mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(X)) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(X)), \qquad \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(Y)) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(Y))$$

позволяют рассматривать $V_\ell(X)$ и $V_\ell(Y)$ как представления группы $\mathrm{Gal}(K)$ над полем $\mathbb{Q}_\ell$.

В-третьих, я утверждаю, что естественное представление группы $\mathrm{Gal}(K)$ в векторном пространстве $\mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(Y), V_\ell(X))$ над $\mathbb{Q}_\ell$ является неприводимым. Действительно, $\mathbb{Z}_\ell$-модуль $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(Y), T_\ell(X))$ является $\mathrm{Gal}(K)$-инвариантной решеткой в $\mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(Y), V_\ell(X))$. С другой стороны, редукция этой решетки по модулю ℓ есть

$$\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(Y), T_\ell(X)) \otimes \mathbb{Z}/\ell\mathbb{Z} = \mathrm{Hom}_{\mathbb{F}_\ell}(T_\ell(Y)/\ell T_\ell(Y), T_\ell(X)/\ell T_\ell(X)) = \mathrm{Hom}_{\mathbb{F}_\ell}(Y_\ell, X_\ell).$$

Но мы только что убедились в простоте $\mathrm{Gal}(K)$-модуля $\mathrm{Hom}_{\mathbb{F}_\ell}(Y_\ell, X_\ell)$. Отсюда легко вытекает простота $\mathrm{Gal}(K)$-модуля $\mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(X), V_\ell(Y))$ (см., например, упражнение 2 в §15.2 книги Серра [18]).

В-четвертых, заметим, что определено естественное вложение [14, §19]

$$\mathrm{Hom}(Y, X) \otimes \mathbb{Q}_\ell \subset \mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(Y), V_\ell(X)),$$

образ которого является $\mathrm{Gal}(K)$-инвариантным подпространством. Из неприводимости пространства $\mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(Y), V_\ell(X))$ вытекает, что либо

$$\mathrm{Hom}(Y, X) \otimes \mathbb{Q}_\ell = \mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(Y), V_\ell(X)),$$

либо $\mathrm{Hom}(Y, X) \otimes \mathbb{Q}_\ell = 0$. Поскольку $\mathrm{Hom}(Y, X)$ — свободная коммутативная группа конечного ранга, то либо $\mathrm{Hom}(Y, X) = 0$, либо ранг группы $\mathrm{Hom}(Y, X)$ равен $4\dim(X) \cdot \dim(Y)$. Для окончания доказательства нам понадобится следующее

Предложение 3.3. *Пусть A и B — абелевы многообразия положительной размерности над алгебраически замкнутым полем $\mathcal{K}$. Предположим, что ранг группы $\mathrm{Hom}(A, B)$ равен $4\dim(A) \cdot \dim(B)$. Тогда $\mathrm{char}(\mathcal{K}) > 0$ и оба многообразия A и B суперсингулярны.*

Доказательство. Случай $A = B$ разобран в лемме 3.1 работы [20].

Заменив абелевы многообразия A и B на изогенные, мы можем считать, что они разлагаются в конечные произведения

$$A = \prod_i A_i, \qquad B = \prod_j B_j$$

простых абелевых многообразий A_i и B_j соответственно. Поскольку

$$\dim(A) = \sum_i \dim(A_i), \qquad \dim(B) = \sum_j \dim(B_j), \qquad \mathrm{Hom}(A, B) = \prod_{i,j} \mathrm{Hom}(A_i, B_j)$$

и ранг свободной коммутативной группы $\mathrm{Hom}(A_i, B_j)$ не превосходит $4\dim(A_i) \cdot \dim(B_j)$ [14, §19, Corollary 1 to Theorem 3], то ранг группы $\mathrm{Hom}(A_i, B_j)$ равен $4\dim(A_i) \cdot \dim(B_j)$ для всех i и j. Поскольку A_i и B_j просты, то они изогенны. Отсюда вытекает, что $\dim(A_i) = \dim(B_j)$ и ранг каждой из свободных коммутативных (относительно сложения) групп $\mathrm{End}(A_i)$ и $\mathrm{End}(B_j)$ равен

$$4\dim(A_i) \cdot \dim(B_j) = 4\dim(A_i)^2 = 4\dim(B_j)^2.$$

Применяя лемму 3.1 работы [20] к каждому из A_i и B_j, мы заключаем, что $\mathrm{char}(\mathcal{K}) > 0$ и все A_i и B_j суперсингулярны. Отсюда легко вытекает суперсингулярность A и B. □

Окончание доказательства теоремы 2.1. Применяя предложение 3.3 к $A = Y$ и $B = X$, мы заключаем, что $\mathrm{char}(K) > 0$, а X и Y суперсингулярны. □

Доказательство леммы 3.1. В течение всего доказательства все рассматриваемые тензорные произведения берутся над полем F. Прежде всего, заменив H_1-модуль W_1 на двойственный $W_1^* = \mathrm{Hom}_F(W_1, F)$, мы сводим задачу к утверждению о неприводимости тензорного произведения

$$\tau_1 \otimes \tau_2 \colon\ H_1 \times H_2 \to \mathrm{Aut}_F(W_1 \otimes W_2).$$

Поскольку H_2-модуль W_2 абсолютно прост, то отвечающий τ_2 гомоморфизм F-алгебр

$$F[H_2] \to \mathrm{End}_F(W_2)$$

сюръективен. Здесь $F[H_2]$ — групповая алгебра группы H_2.

Обозначим через D кольцо эндоморфизмов $F[H_1]$-модуля W_1. Поскольку W_1 прост, D — тело, центр которого содержит F. Ясно, что размерность D над F конечна и что W_2 — свободный D-модуль конечного ранга. Из теоремы плотности Джекобсона вытекает, что образ отвечающего τ_2 гомоморфизма F-алгебр

$$F[H_1] \to \mathrm{End}_F(W_1)$$

совпадает с $\mathrm{End}_D(W_1)$. Здесь $F[H_1]$ — групповая алгебра группы H_1. На $W_1 \otimes W_2$ определена естественная структура свободного $D \otimes F = D$-модуля конечного ранга. Ясно, что $\mathrm{End}_D(W_1 \otimes W_2)$-модуль $W_1 \otimes W_2$ прост.

Отсюда вытекает, что образ отвечающего $\tau_1 \otimes \tau_2$ гомоморфизма F-алгебр

$$F[H_1 \times H_2] = F[H_1] \otimes F[H_2] \to \mathrm{End}_F(W_1 \otimes W_2)$$

совпадает с $\mathrm{End}_D(W_1) \otimes \mathrm{End}_F(W_2)$. Из леммы 10.37 на с. 252 книги [2] вытекает, что

$$\mathrm{End}_D(W_1) \otimes \mathrm{End}_F(W_2) = \mathrm{End}_{D \otimes F}(W_1 \otimes W_2).$$

Следовательно, образ групповой алгебры $F[H_1 \times H_2]$ в $\mathrm{End}_F(W_1 \otimes W_2)$ совпадает с

$$\mathrm{End}_{D \otimes F}(W_1 \otimes W_2) = \mathrm{End}_D(W_1 \otimes W_2).$$

Теперь простота $\mathrm{End}_D(W_1 \otimes W_2)$-модуля $W_1 \otimes W_2$ влечет за собой простоту $F[H_1 \times H_2]$-модуля $W_1 \otimes W_2$. $\square$

4. ДОКАЗАТЕЛЬСТВО СЛЕДСТВИЙ 1.4 И 1.5

Мы начнем со следующего полезного определения.

Определение 4.1. Мы называем конечные группы G_1 и G_2 *разделенными*, если у них нет изоморфных фактор-групп, за исключением тривиальной одноэлементной группы.

Примеры 4.2. Легко видеть, что следующие пары доставляют примеры разделенных групп:

(i) $\mathbf{S}_3$ и $\mathbf{A}_3$;

(ii) $\mathbf{S}_n$ и $\mathbf{A}_m$, $m \geq 5$;

(iii) $\mathbf{A}_n$ и $\mathbf{A}_m$, $n \neq m$ и $m \geq 5$;

(iv) $G_1 := \mathrm{PSL}(d, q) \subset G_2 := \mathrm{PGL}(d, q)$, где

  (a) $d > 1$, $(d, q) \neq (2, 2)$, $(d, q) \neq (2, 3)$;

  (b) числа d и $q - 1$ имеют *нетривиальный* общий делитель.

Условие (a) означает, что G_1 — простая конечная неабелева группа [19, Ch. 1, §9], а условие (b) — что $G_1 \neq G_2$. Ясно, что G_1 — нормальная подгруппа в G_2 и фактор-группа G_2/G_1 — циклическая группа порядка r, где r — наибольший общий делитель чисел d и $q-1$. Чтобы убедиться в том, что G_1 и G_2 разделены, достаточно проверить, что не существует сюръективного гомоморфизма $\phi\colon G_2 \twoheadrightarrow G_1$. Предположим, что такой гомоморфизм существует. Тогда его ядро $\ker(\phi)$ — собственная нормальная подгруппа в $G_2 = \mathrm{PGL}(d,q)$ и ее прообраз G' в $\mathrm{GL}(d,q)$ — собственная нормальная подгруппа группы $\mathrm{GL}(d,q)$, содержащая все скаляры, а также некоторый элемент, не являющийся скаляром. Поскольку любая нормальная подгруппа в $\mathrm{GL}(d,q)$ либо содержит $\mathrm{SL}(d,q)$, либо содержится в группе скаляров [19, Ch. 1, §9, Theorem 9.9], мы заключаем, что G' содержит $\mathrm{SL}(d,q)$ и, следовательно, $\ker(\phi)$ содержит $\mathrm{PSL}(d,q) = G_1$. Отсюда вытекает, что образ G_1 сюръективного гомоморфизма ϕ изоморфен фактор-группе циклической группы G_2/G_1 и, следовательно, также является циклической группой. Неабелевость группы $G_1 := \mathrm{PSL}(d,q)$ доставляет желаемое противоречие, которое и доказывает разделенность групп G_1 и G_2.

Напомним формулировку хорошо известной леммы Гурса (см., например, [10, p. 75]).

Лемма 4.3. *Пусть G_1 и G_2 — конечные группы. Пусть H — подгруппа в произведении $G_1 \times G_2$ такая, что соответствующие отображения проекции $\mathrm{pr}_1\colon H \to G_1$ и $\mathrm{pr}_2\colon H \to G_2$ сюръективны. Обозначим через H_1 (соответственно H_2) нормальную подгруппу в G_1 (соответственно G_2) такую, что ядро гомоморфизма pr_2 (соответственно pr_1) совпадает с $H_1 \times \{1\}$ (соответственно $\{1\} \times H_2$). Тогда существует изоморфизм факторгрупп $\gamma\colon G_1/H_1 \cong G_2/H_2$ такой, что H совпадает с прообразом в $G_1 \times G_2$ графика γ в $G_1/H_1 \times G_2/H_2$.*

Замечания 4.4. (i) Если $H_1 = G_1$, $H_2 = G_2$, то $H = G_1 \times G_2$. А если $H_1 = \{1\}$, $H_2 = \{1\}$, то $G_1 \cong G_2 \cong G$.

(ii) Если G_1 и G_2 — разделенные конечные группы, то легко видеть, что любая подгруппа в произведении $G_1 \times G_2$, сюръективно отображающаяся на каждый из факторов, совпадает с $G_1 \times G_2$.

(iii) Если $G_1 = G_2 = G$ — конечная простая группа, то легко видеть, что либо $H_1 = G_1$, $H_2 = G_2$ и $H = G_1 \times G_2$, либо $H_1 = \{1\}$, $H_2 = \{1\}$ и $G_1 \cong G_2 \cong G$.

Предложение 4.5. *Пусть K — поле характеристики, отличной от 2, а K_a — его алгебраическое замыкание. Пусть $f(x), h(x) \in K[x]$ — неприводимые многочлены без кратных корней степени $n \geq 3$ и $m \geq 3$ соответственно. Пусть группы Галуа $\mathrm{Gal}(f)$ и $\mathrm{Gal}(h)$ многочленов f и h разделены. Предположим, что многочлен $f(x)$ очень хорош, а многочлен $h(x)$ хорош.*

Тогда либо

$$\mathrm{Hom}(J(C_f), J(C_h)) = 0, \qquad \mathrm{Hom}(J(C_h), J(C_f)) = 0,$$

либо $\mathrm{char}(K) > 0$ и оба якобиана $J(C_f)$ и $J(C_h)$ — суперсингулярные абелевы многообразия.

Доказательство. Пусть $K(\mathfrak{R}_f)$ и $K(\mathfrak{R}_h)$ — поля разложения многочленов f и h соответственно, а L — композит полей $K(\mathfrak{R}_f)$ и $K(\mathfrak{R}_h)$. Тогда группа Галуа $\mathrm{Gal}(L/K)$ расширения L/K естественным образом отождествляется с подгруппой произведения $\mathrm{Gal}(f) \times \mathrm{Gal}(h)$, сюръективно отображающейся (при отображениях проекции) на каждый из факторов $\mathrm{Gal}(f)$ и $\mathrm{Gal}(h)$. Из замечания 4.4(ii) и разделенности групп $\mathrm{Gal}(f)$ и $\mathrm{Gal}(h)$ вытекает, что подгруппа $\mathrm{Gal}(L/K)$ совпадает с произведением $\mathrm{Gal}(f) \times \mathrm{Gal}(h)$. Это означает, что расширения $K(\mathfrak{R}_f)$ и $K(\mathfrak{R}_h)$ линейно разделены над K, и утверждение предложения 4.5 немедленно вытекает из теоремы 1.2. $\square$

Доказательство следствия 1.4. Из теоремы 1.1 вытекает, что $\mathrm{End}(J(C_f)) = \mathbb{Z}$. Следовательно, если $\mathrm{Hom}(J(C_f), J(C_h)) \neq 0$, то $\dim(J(C_h)) \geq \dim(J(C_f))$. Отсюда вытекает, что $\deg(h) \geq 5$, а если $\mathrm{char}(K) > 0$, то $m = \deg(h) \geq 9$. Повторное применение теоремы 1.1 дает нам равенство $\mathrm{End}(J(C_h)) = \mathbb{Z}$. Отсюда вытекает, что если $\mathrm{Hom}(J(C_f), J(C_h)) \neq 0$, то $\dim(J(C_h)) = \dim(J(C_f))$. Последнее равенство означает, что либо $n = m$, либо n четно и $m = n - 1$, либо m четно и $n = m - 1$.

Далее, заменив в случае, когда $n \neq m$ и $\mathrm{Gal}(f) = \mathbf{S}_n$, поле K на соответствующее квадратичное или биквадратичное расширение, мы можем считать, что либо

$$n \neq m, \qquad \mathrm{Gal}(f) = \mathbf{A}_n, \qquad \mathrm{Gal}(h) = \mathbf{A}_m,$$

либо

$$n = m, \qquad \mathrm{Gal}(f) = \mathbf{S}_n, \qquad \mathrm{Gal}(h) = \mathbf{A}_m = \mathbf{A}_n.$$

Отметим, что в обоих случаях группы $G_1 := \mathrm{Gal}(f)$ и $G_2 := \mathrm{Gal}(h)$ разделены. Остается применить предложение 4.5. $\square$

Для доказательства следствия 1.5 нам понадобится некоторое элементарное утверждение из теории Галуа. Но вначале введем следующие обозначения. Пусть L/K — поле разложения сепарабельного многочлена $f(x) \in K[x]$ степени n. Тогда множество корней $\mathfrak{R}_f$ многочлена f лежит в поле L и порождает его над K, что дает нам естественное вложение $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Perm}(\mathfrak{R}_f)$, которое мы обозначим через r_f. С другой стороны, любая нумерация $\{\alpha_1, \ldots, \alpha_n\}$ элементов $\mathfrak{R}_f$ (т.е. корней f) позволяет отождествить $\mathrm{Perm}(\mathfrak{R}_f)$ и $\mathbf{S}_n$ и мы можем рассматривать r_f как гомоморфизм

$$r_f\colon\ \mathrm{Gal}(L/K) \hookrightarrow \mathrm{Perm}(\mathfrak{R}_f) = \mathbf{S}_n.$$

Отметим, что для любого натурального числа $j \leq n$ стабилизатор $\mathrm{Gal}(L/K)_{\alpha_j}$ корня α_j в группе $\mathrm{Gal}(L/K)$ совпадает с прообразом $r_f^{-1}(\mathbf{S}_n^{\{j\}})$ подгруппы $\mathbf{S}_n^{\{j\}}$, состоящей из всех перестановок, оставляющих на месте число j.

Лемма 4.6. *Предположим, что конечное расширение Галуа L/K, натуральное число n и транзитивная группа перестановок $\Gamma \subset \mathbf{S}_n$ удовлетворяют следующим условиям*:

(i) *если $\mathrm{Gal}(L/K)$ — группа Галуа расширения L/K, то существует вложение $\mathrm{Gal}(L/K) \hookrightarrow \mathbf{S}_n$, образ которого совпадает с Γ;*

(ii) *для любого автоморфизма $u\colon \Gamma \to \Gamma$ группы Γ найдется перестановка $s \in \mathbf{S}_n$ такая, что $u(z) = szs^{-1}$ $\forall z \in \Gamma$.*

Предположим, что $f(x), h(x) \in K[x]$ — два сепарабельных (т.е. без кратных корней) неприводимых многочлена степени n такие, что L является полем разложения каждого из них. Предположим дополнительно, что можно так перенумеровать корни $\{\alpha_1, \ldots, \alpha_n\}$ многочлена f и корни $\{\beta_1, \ldots, \beta_n\}$ многочлена h, что образ каждого из естественных гомоморфизмов

$$r_f\colon\ \mathrm{Gal}(L/K) \hookrightarrow \mathrm{Perm}(\mathfrak{R}_f) = \mathbf{S}_n, \qquad r_h\colon\ \mathrm{Gal}(L/K) \hookrightarrow \mathrm{Perm}(\mathfrak{R}_h) = \mathbf{S}_n$$

совпадает с Γ.

Тогда если α — корень многочлена f, то найдется корень $\beta \in L$ многочлена h такой, что $K(\alpha) = K(\beta)$.

Доказательство. Легко видеть, что $\mathrm{Gal}(L/K) \cong \Gamma$ и найдется перестановка $s \in \mathbf{S}_n$ такая, что

$$r_h(\sigma) = s r_f(\sigma) s^{-1} \qquad \forall \sigma \in \mathrm{Gal}(L/K).$$

Если $j = s(i)$, то легко видеть, что

$$r_h^{-1}(\mathbf{S}_n^{\{j\}}) = r_f^{-1}(\mathbf{S}_n^{\{i\}})$$

и, следовательно, в группе Галуа $\mathrm{Gal}(L/K)$ стабилизатор $\mathrm{Gal}(L/K)_{\beta_j}$ корня β_j совпадает со стабилизатором $\mathrm{Gal}(L/K)_{\alpha_j}$ корня α_j. Это значит, что $K(\alpha_i) = K(\beta_j)$. $\square$

Доказательство следствия 1.5. Ввиду следствия 1.4 мы можем предположить, что либо

$$\mathrm{Gal}(f) = \mathbf{S}_n, \qquad \mathrm{Gal}(h) = \mathbf{S}_n,$$

либо

$$\mathrm{Gal}(f) = \mathbf{A}_n, \qquad \mathrm{Gal}(h) = \mathbf{A}_n.$$

Предположим, что нормальные расширения полей $K(\mathfrak{R}_f)$ и $K(\mathfrak{R}_h)$ *не* совпадают (неизоморфны). Тогда их композит L не совпадает ни с $K(\mathfrak{R}_f)$, ни с $K(\mathfrak{R}_h)$ и, следовательно, $\mathrm{Gal}(L/K)$ неизоморфна ни $\mathrm{Gal}(f)$, ни $\mathrm{Gal}(h)$. Применяя замечание 4.4(iii) к $H = \mathrm{Gal}(L/K)$, $G_1 = \mathrm{Gal}(f)$ и $G_2 = \mathrm{Gal}(h)$, мы получаем, что если $\mathrm{Gal}(f) = \mathbf{A}_n$, $\mathrm{Gal}(h) = \mathbf{A}_n$, то $\mathrm{Gal}(L/K) = \mathrm{Gal}(f) \times \mathrm{Gal}(h)$, поскольку $H = \mathrm{Gal}(L/K)$ неизоморфна $G_1 = \mathrm{Gal}(f)$. Следовательно, $K(\mathfrak{R}_f)$ и $K(\mathfrak{R}_h)$ линейно разделены над K и утверждение доказываемого следствия немедленно вытекает из теоремы 1.2. Если же $\mathrm{Gal}(f) = \mathbf{S}_n$, $\mathrm{Gal}(h) = \mathbf{S}_n$, то быстрый взгляд на список всех фактор-групп группы $\mathbf{S}_n$ позволяет нам, применяя лемму 4.3 к $H = \mathrm{Gal}(L/K)$, $G_1 = \mathrm{Gal}(f)$ и $G_2 = \mathrm{Gal}(h)$, получить, что либо $\mathrm{Gal}(L/K) = \mathrm{Gal}(f) \times \mathrm{Gal}(h)$ и утверждение доказываемого следствия вытекает из теоремы 1.2, либо $\mathrm{Gal}(L/K)$ совпадает со следующей подгруппой индекса 2 в $\mathrm{Gal}(f) \times \mathrm{Gal}(h) = \mathbf{S}_n \times \mathbf{S}_n$, содержащей $\mathbf{A}_n \times \mathbf{A}_n$:

$$\{(\sigma, \tau) \in \mathbf{S}_n \times \mathbf{S}_n \mid \mathrm{sign}(\sigma) = \mathrm{sign}(\tau)\}.$$

(Здесь $\mathrm{sign}(\sigma)$ — знак перестановки σ.) Заменив (в последнем случае) поле K на соответствующее квадратичное расширение, мы можем считать, что

$$\mathrm{Gal}(L/K) = \mathbf{A}_n \times \mathbf{A}_n, \qquad \mathrm{Gal}(f) = \mathbf{A}_n, \qquad \mathrm{Gal}(h) = \mathbf{A}_n,$$

и те же аргументы, что и в предыдущем случае, доказывают следствие 1.5. Значит, для доказательства следствия 1.5 достаточно убедиться в *несовпадении* расширений $K(\mathfrak{R}_f)$ и $K(\mathfrak{R}_h)$, чем мы сейчас и займемся.

Предположим, что $K(\mathfrak{R}_f) = K(\mathfrak{R}_h)$. Заменив K на соответствующее квадратичное или биквадратичное расширение, мы можем считать, что

$$\mathrm{Gal}(f) = \mathbf{A}_n, \qquad \mathrm{Gal}(h) = \mathbf{A}_n.$$

Положим $L = K(\mathfrak{R}_f) = K(\mathfrak{R}_h)$. Ясно, что $\mathrm{Gal}(L/K) \cong \mathbf{A}_n$. Напомним, что если $n \geq 5$ и $n \neq 6$, то $\mathrm{Aut}(\mathbf{A}_n) = \mathbf{S}_n$ [19, §2.17, p. 299–300]. Применяя лемму 4.6, мы заключаем, что $K(\alpha) = K(\beta)$ для некоторых корней α многочлена f и β многочлена h. Однако $K(\alpha) \cong K[x]/fK[x] = K_f$ и $K(\beta) \cong K[x]/hK[x] = K_h$. Следовательно, расширения полей K_f/K и K_h/K изоморфны. Противоречие. $\square$

5. ПРИМЕРЫ

Обозначим через $\overline{\mathbb{Q}}$ (алгебраически замкнутое) поле всех алгебраических чисел в $\mathbb{C}$.

Положим $f_n(x) = x^n - x - 1 \in \mathbb{Q}[x]$ и рассмотрим числовое поле $E_n = \mathbb{Q}[x]/f_n\mathbb{Q}[x]$. Согласно Серру [17, p. 45, Remark 2] для любого натурального n группа Галуа многочлена $f_n(x) = x^n - x - 1$ над полем рациональных чисел $\mathbb{Q}$ равна $\mathbf{S}_n$. Там же доказано, что для любого простого числа p либо многочлен $\widetilde{f}_n(x) := x^n - x - 1 \in \mathbb{F}_p[x]$ не имеет кратных корней,

либо p не делит $n(n-1)$ и

$$\widetilde{f}_n(x) = \left(x - \frac{n}{1-n}\right)^2 \widetilde{w}(x),$$

где многочлен $\widetilde{w}(x) \in \mathbb{F}_p[x]$ не имеет кратных корней и $0 \neq \widetilde{w}(\frac{n}{1-n}) \in \mathbb{F}_p$. Ясно, что если $\widetilde{f}_n$ не имеет кратных корней, то по лемме Гензеля $f_n(x)$ разлагается на линейные множители над неразветвленным расширением поля $\mathbb{Q}_p$ и, следовательно, расширение $E_n/\mathbb{Q}$ не разветвлено над p. Если же $\widetilde{f}_n$ имеет кратный корень, то многочлены $\widetilde{w}(x)$ и $(x - \frac{n}{1-n})^2$ взаимно просты в $\mathbb{F}_p(x)$ и согласно известному обобщению леммы Гензеля [6, §3.5, p. 105] многочлен $f_n(x)$ разлагается над $\mathbb{Q}_p$ в произведение квадратичного многочлена (являющегося подъемом $(x - \frac{n}{1-n})^2$) и многочлена $w(x)$ (являющегося подъемом $\widetilde{w}(x)$), причем $w(x)$ разлагается на линейные множители над неразветвленным расширением поля $\mathbb{Q}_p$. Отсюда вытекает, что если расширение $E_n/\mathbb{Q}$ разветвлено над p, то только в одном простом идеале кольца целых поля E_n и соответствующий индекс ветвления равен 2.

Рассмотрим гиперэллиптическую кривую $A_n\colon y^2 = f_n(x)$, определенную над $\mathbb{Q}$, и ее якобиан $J(A_n)$. Если $n \leq 4$, то $J(A_n)$ — эллиптическая кривая, а если $n \geq 5$, то $\operatorname{End}(J(A_n)) = \mathbb{Z}$ [20]. Тем самым абелево многообразие $J(A_n)$ всегда абсолютно просто. Из следствия 1.4 вытекает, что если $n \geq 5$, $m \geq 3$ и $n \neq m$, то любой гомоморфизм между соответствующими якобианами $J(A_n)$ и $J(A_m)$, определенный над $\overline{\mathbb{Q}}$, равен нулю. Отсюда немедленно вытекает, что любой гомоморфизм между якобианами $J(A_n)$ и $J(A_m)$, определенный над полем комплексных чисел $\mathbb{C}$, равен нулю. (Конечно, здесь единственный интересный случай — это когда $n = 2g+1$ нечетно, а $m = 2g+2$ четно и абсолютно простые абелевы многообразия $J(A_{2g+1})$ и $J(A_{2g+2})$ имеют одну и ту же размерность g.)

Согласно Шуру [15] группа Галуа $\operatorname{Gal}(\exp_n)$ многочлена

$$\exp_n(x) := 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \ldots + \frac{x^n}{n!}$$

над полем рациональных чисел $\mathbb{Q}$ равна $\mathbf{S}_n$, если n не делится на 4; если $4 \mid n$, то $\operatorname{Gal}(\exp_n) = \mathbf{A}_n$. Рассмотрим гиперэллиптическую кривую $B_n\colon y^2 = f_n(x)$, определенную над $\mathbb{Q}$, и ее якобиан $J(B_n)$. Если $n \leq 4$, то $J(B_n)$ — эллиптическая кривая, а если $n \geq 5$, то $\operatorname{End}(J(B_n)) = \mathbb{Z}$ [20]. Тем самым абелево многообразие $J(B_n)$ всегда абсолютно просто. Из следствия 1.4 вытекает, что если $n \geq 5$, $m \geq 3$ и $n \neq m$, то любой гомоморфизм между соответствующими якобианами $J(B_n)$ и $J(B_m)$, а также между $J(B_n)$ и $J(A_m)$, определенный над $\overline{\mathbb{Q}}$ или (что то же самое) над $\mathbb{C}$, равен нулю. Также из следствия 1.4 вытекает, что если $n > 5$ и $4 \mid n$, то любой гомоморфизм между $J(B_n)$ и $J(A_n)$ равен нулю.

Докажем, используя следствие 1.5, что для всех $n > 6$ любой гомоморфизм между $J(B_n)$ и $J(A_n)$ равен нулю. Для этого рассмотрим числовое поле $H_n = \mathbb{Q}[x]/\exp_n \mathbb{Q}[x]$. Наша цель будет достигнута, если мы докажем, что поля E_n и H_n неизоморфны. Для этого с помощью теоремы Чебышева (постулата Бертрана) выберем простое число p, удовлетворяющее неравенствам

$$g + 1 \leq p \leq 2g + 1,$$

где либо $n = 2g+1$ нечетно, либо $n = 2g+2$ четно. В частности,

$$p \geq g + 1 \geq \frac{n}{2} > 3.$$

Обозначим через

$$\operatorname{ord}_p\colon \mathbb{Q}^* \to \mathbb{Z}$$

отвечающее простому p дискретное нормирование поля $\mathbb{Q}$, нормализованное условием $\operatorname{ord}_p(p) = 1$ [8]. Легко видеть, что для всех натуральных чисел $i < p$

$$\operatorname{ord}_p\left(\frac{1}{i!}\right) = 0,$$

а для всех целых i, удовлетворяющих неравенству $p \le i \le n$,

$$\operatorname{ord}_p\left(\frac{1}{i!}\right) = -1,$$

за исключением случая

$$n = 2g + 2 = i, \qquad p = g + 1, \qquad \operatorname{ord}_p\left(\frac{1}{i!}\right) = \operatorname{ord}_{g+1}\left(\frac{1}{(2g+2)!}\right) = -2.$$

Отсюда вытекает, что рациональное число $-\frac{1}{p}$ является *наклоном* p-адического многоугольника Ньютона многочлена $\exp_n(x)$. Известная связь между (обратными) корнями многочлена и наклонами его многоугольника Ньютона [8] позволяет заключить, что для некоторого простого идеала в кольце целых поля H_n, лежащего над p, соответствующий индекс ветвления делится на $p > 3$. Поскольку все индексы ветвления расширения $E_n/\mathbb{Q}$ не превосходят 2 (см. начало этого раздела), поля E_n и H_n неизоморфны. Применяя следствие 1.5 к $f = f_n$, $h = \exp_n$, мы заключаем, что для всех $n > 6$ любой гомоморфизм между $J(B_n)$ и $J(A_n)$, определенный над $\overline{\mathbb{Q}}$ или (что то же самое) над $\mathbb{C}$, равен нулю.

Обратимся теперь к совершенно другому классу примеров. Пусть p — нечетное простое число, k_p — алгебраически замкнутое поле характеристики p, $K = K(t)$ — поле рациональных функций от независимой переменной t с коэффициентами в k_p, а K_a — алгебраическое замыкание поля K. Пусть целое $q > 1$ — степень числа p, $d > 1$ — натуральное число. Положим

$$n = \frac{q^d - 1}{q - 1} = \#(\mathbf{P}^{d-1}(\mathbb{F}_q))$$

и рассмотрим многочлены

$$f(x) = x^n + tx + 1 \in K[x], \qquad h(x) = x^n + x + t \in K[x].$$

Согласно Абъянкару [1] существуют биекции

$$\mathfrak{R}_f \cong \mathbf{P}^{d-1}(\mathbb{F}_q), \qquad \mathfrak{R}_h \cong \mathbf{P}^{d-1}(\mathbb{F}_q)$$

такие, что группа $\operatorname{Gal}(f)$ превращается в $\operatorname{PSL}(d, q)$, а группа $\operatorname{Gal}(h)$ превращается в $\operatorname{PGL}(d, q)$. Предположим дополнительно, что $m > 2$. Тогда оба многочлена $f(x)$ и $h(x)$ очень хороши. Также предположим, что числа d и $q - 1$ *не* взаимно просты. Тогда группы Галуа $\operatorname{Gal}(f) = \operatorname{PSL}(d, q)$ и $\operatorname{Gal}(h) = \operatorname{PGL}(d, q)$ разделены (см. пример 4.2(iv)). Согласно предложению 4.5 если $J(C_f)$ и $J(C_h)$ — якобианы гиперэллиптических кривых

$$C_f\colon\ y^2 = f(x), \qquad C_h\colon\ y^2 = h(x),$$

то либо оба якобиана суперсингулярны, либо любой гомоморфизм между $J(C_f)$ и $J(C_h)$, определенный над K_a, равен нулю. Но согласно теореме 2.4(iv) работы [23] если $(q, d) \ne (3, 4)$, то

$$\operatorname{End}(J(C_f)) = \mathbb{Z}, \qquad \operatorname{End}(J(C_h)) = \mathbb{Z}$$

и, следовательно, оба якобиана несуперсингулярны. Следовательно, если $(q, d) \ne (3, 4)$, то любой гомоморфизм между $J(C_f)$ и $J(C_h)$, определенный над K_a, равен нулю.

СПИСОК ЛИТЕРАТУРЫ

1. *Abhyankar S.S.* Projective polynomials // Proc. Amer. Math. Soc. 1997. V. 125, N 6. P. 1643–1650.
2. *Curtis Ch.W., Reiner I.* Methods of representation theory. New York: J. Wiley & Sons; Toronto: Chichester Brisbane, 1981. V. 1.
3. *Dixon J.D., Mortimer B.* Permutation groups. New York; Berlin; Heidelberg: Springer, 1996.
4. *Huppert B.* Endliche Gruppen. I. Berlin; Heidelberg; New York: Springer, 1967.
5. *Huppert B., Blackburn N.* Finite groups. III. Berlin; Heidelberg; New York: Springer, 1982.
6. *Janusz G.J.* Algebraic number fields. 2nd ed. Providence (RI): Amer. Math. Soc., 1996.
7. *Klemm M.* Über die Reduktion von Permutationsmoduln // Math. Ztschr. 1975. Bd. 143. S. 113–117.
8. *Koblitz N.* p-Adic numbers, p-adic analysis, and zeta-functions. Berlin; Heidelberg; New York: Springer, 1977.
9. *Ivanov A.A., Praeger Ch.E.* On finite affine 2-arc transitive graphs // Europ. J. Comb. 1993. V. 14, N 5. P. 421–444.
10. *Lang S.* Algebra. 3rd ed. Reading (MA): Addison–Wesley, 1993.
11. *Mori Sh.* The endomorphism rings of some abelian varieties. II // Japan. J. Math. 1977. V. 3. P. 105–109.
12. *Mortimer B.* The modular permutation representations of the known doubly transitive groups // Proc. London Math. Soc. Ser. 3. 1980. V. 41. P. 1–20.
13. *Mumford D.* Theta characteristics of an algebraic curve // Ann. Sci. École Norm. Supér. Sér. 4. 1971. V. 4. P. 181–192.
14. *Mumford D.* Abelian varieties. 2nd ed. London: Oxford Univ. Press, 1974.
15. *Schur I.* Gleichungen ohne Affect // Sitzungsber. Preuss. Akad. Wiss. Phys.-Math. Kl. 1930. S. 443–449. То же: Ges. Abh. Bd. 3. S. 191–197.
16. *Serre J.-P.* Lectures on the Mordell–Weil theorem. 2nd ed. Braunschweig; Wiesbaden: F. Vieweg & Sohn, 1989.
17. *Serre J.-P.* Topics in Galois theory. Boston; London: Jones and Bartlett Publ., 1992.
18. *Serre J.-P.* Représentations linéaires des groupes finis. 3me éd. Paris: Hermann, 1978.
19. *Suzuki M.* Group theory. I. Berlin; Heidelberg; New York: Springer, 1982.
20. *Zarhin Yu.G.* Hyperelliptic Jacobians without complex multiplication // Math. Res. Lett. 2000. V. 7, N 1. P. 123–132.
21. *Zarhin Yu.G.* Hyperelliptic Jacobians and modular representations // Moduli of abelian varieties / Eds. C. Faber, G. van der Geer, F. Oort. Basel; Boston; Berlin: Birkhäuser, 2001. P. 473–490. (Progr. Math.; V. 195).
22. *Zarhin Yu.G.* Hyperelliptic Jacobians without complex multiplication in positive characteristic // Math. Res. Lett. 2001. V. 8, N 4. P. 429–435.
23. *Zarhin Yu.G.* Very simple 2-adic representations and hyperelliptic Jacobians // Moscow Math. J. 2002. V. 2, N 2. P. 403–431.
24. *Zarhin Yu.G.* Hyperelliptic Jacobians and simple groups $\mathrm{U}_3(2^m)$ // Proc. Amer. Math. Soc. 2003. V. 131, N 1. P. 95–102.