D. Oganesyan

ABEL PAIRS AND MODULAR CURVES

ABSTRACT. We consider rational functions on algebraic curves which have a single zero and a single pole. A pair consisting of such a function and a curve is called *Abel pair*; a special case of an Abel pair is a Belyi pair. In this paper, we study moduli spaces of Abel pairs for curves of genus one. In particular, we compute a number of Belyi pairs over the fields $\mathbb C$ and $\overline{\mathbb F_p}$. This approach could be fruitfully used for the study of Hurwitz spaces and modular curves for fields of finite characteristics.

§1. Introduction

In this paper we consider algebraic curves and rational function on them with the divisor of a certain combinatorial type. More specifically, we study pairs (\mathcal{X}, α) , where \mathcal{X} is an algebraic curve and α is a function on it with $\operatorname{div}(\alpha) = nA - nC$. We call such a pair an *Abel pair*. An Abel function has two critical values, 0 and ∞ , of valency n; if it has only one additional critical value it is also a *Belyi function*. One of the main results of this paper is the calculation of the number of Abel–Belyi pairs of a given degree and of genus 1 over \mathbb{C} (Theorem 5.8) and $\overline{\mathbb{F}_p}$ (Theorem 6.3).

The idea of the calculation is to include Abel–Belyi pairs in families of Abel pairs. In these families the Abel–Belyi pairs correspond to zeros of some function on the base of the family. Knowing the multiplicities of these zeros and the degree of this function we count the Abel–Belyi pairs of genus 1. This method also works in positive characteristic and for other types of Belyi pairs. The families used in this construction are interesting in their own right; the bases of these families are modular curves $X_1(n)$.

Similar considerations of such Belyi pairs can be found in [2].

I express my gratitude to my supervisor, George B. Shabat, to Gareth A. Jones, Sergei K. Lando and the participants of the Mechmath MSU seminar "Graphs on surfaces and curves over number fields" for their help and fruitful discussions in carrying out this work. I also thank my reviewer

Key words and phrases: Belyi pairs; dessins d'enfants; Abel pairs; reduction to positive characteristic; embedded graphs; modular curves; elliptic curves.

for his advice and corrections. Supported in part by the Simons Foundation.

§2. ABEL PAIRS

Definition 2.1. An Abel pair is a pair (\mathcal{X}, α) , where \mathcal{X} is a complete smooth algebraic curve over an algebraically closed field \mathbb{k} and α is a rational function on it, whose divisor has the form $\operatorname{div}(\alpha) = nA - nB$, where A, B are two different points of the curve \mathcal{X} . Such a function α will be called an Abel function.

Example 2.2. Consider a family of elliptic curves $y^2 = (1 + kx)^2 - 4x^3$, with *j*-invariant

$$j = -\frac{k^3 \left(k^3 + 24\right)^3}{27 + k^3},$$

where $k \in \mathbb{k} \setminus \{-3\sqrt[3]{1}\}$. It is easy to check that $\alpha := 1 + kx - y$ is an Abel function on it: $\deg \alpha = 3$, $\operatorname{div}(\alpha) = 3A - 3B$, where x(A) = 0, y(A) = 1 and B is the infinite point.

How is this definition related to Abel? Abel described in [1] the type of elliptic integrals of the third kind which can be expressed in terms of elementary functions. These integrals are related to Abel pairs. For Example 2.2 we obtain (with u = 1/x, $v = y/x^2$):

$$\int \frac{(3u+k)du}{\sqrt{(u^2+ku)^2-4u}} = \ln \left(u(u+k)^2 - 2 + (u+k)\sqrt{(ku+u^2)^2-4u} \right) + C$$

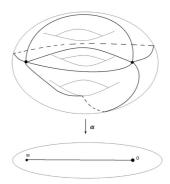
This integration is explained by the fact that the difference of the two infinite points on the curve $v^2 = (u^2 + ku)^2 - 4u$ has order 3.

Definition 2.3. Let $f: \mathcal{X}_1 \to \mathcal{X}_2$ be a morphism of curves and $\lambda \in \mathrm{PSL}_2(\mathbb{k})$. We call a pair $\mathcal{F} = (f, \lambda)$ a morphism from an Abel pair $(\mathcal{X}_1, \alpha_1)$ to an Abel pair $(\mathcal{X}_2, \alpha_2)$ if $\lambda \circ \alpha_1 = \alpha_2 \circ f$, i.e., if the diagram

$$\begin{array}{ccc} X_1 & \stackrel{f}{\longrightarrow} & X_2 \\ & & & & \\ \alpha_1 \Big\downarrow & & & \alpha_2 \Big\downarrow \\ & \mathbb{P}^1(\Bbbk) & \stackrel{\lambda}{\longrightarrow} & \mathbb{P}^1(\Bbbk) \end{array}$$

is commutative.

Remark 2.4. So, pairs (\mathcal{X}, α) , $(\mathcal{X}, 5\alpha)$ (for char $\mathbb{k} \neq 5$) and $(\mathcal{X}, 1/\alpha)$ are isomorphic.



Definition 2.5. We call an Abel pair (\mathcal{X}, α) an Abel-Belyi pair if it is also a Belyi pair, i.e., if α has only three critical values.

The dessin d'enfant $\beta^{-1}([0,1])$ on \mathcal{X} is associated with a Belyi pair (\mathcal{X},β) over the field \mathbb{C} . We color vertices in $\beta^{-1}(0)$ black and vertices in $\beta^{-1}(1)$ white, see [6].

The dessin corresponding to an Abel–Belyi pair has one black vertex and one face.

§3. The embedded graph associated with an Abel Pair

Let (\mathcal{X}, α) be an Abel pair. Define

$$\Gamma_{\mathcal{X},\alpha} := \alpha^{-1}(\mathbb{R}_{\leq 0} \cup {\infty}) \subset \mathcal{X}.$$

Proposition 3.1. If α has no critical values on the half-line $\mathbb{R}_{<0}$, then $\Gamma_{\mathcal{X},\alpha}$ is embedded in \mathcal{X} ; this graph has two vertices and $n = \deg \alpha$ edges.

This embedding is not necessarily a dessin because some of its faces may not be simply-connected. For example, for the pair (\mathcal{X}, α) , where \mathcal{X} is given by the equation $y^2 = x^3 + x$ and $\alpha = x$, $\Gamma_{\mathcal{X},\alpha}$ is not a dessin since the complement $\mathcal{X} \setminus \Gamma_{\mathcal{X},\alpha}$ is homeomorphic to a cylinder.

Next we consider the combinatorics of these embedded graphs. The semi-edges incident with the vertex $\alpha^{-1}(0)$ are cyclically ordered, and the same is true for $\alpha^{-1}(\infty)$. The edges of this graph define a bijection between two cyclically ordered n-element sets of semi-edges. By counting the number of such bijections we get the following proposition (where Abel–Belyi pairs are counted with weight 1/#Aut):

Proposition 3.2. The number of Abel-Belyi pairs of degree n is

$$m(n) = \sum_{\deg \alpha = n} \frac{1}{\# Aut(\mathcal{X}, \alpha)} = \frac{(n-1)!}{n}.$$

In the above proposition we have counted all the Abel–Belyi pairs of a fixed degree, and of all possible genera. Next we want to separate them according to their genus and the list of their valencies. We also want to establish similar formulae in positive characteristic, so we undertake some algebraic considerations.

§4. Defining equations of Abel curves

Let \mathcal{X} be an irreducible algebraic curve over \mathbb{k} and $\alpha \in \mathbb{k}[\mathcal{X}]$ a function on it, with deg $\alpha = n$ and char $\mathbb{k} \nmid n$. Note that \mathcal{X} may be singular.

Theorem 4.1. Suppose that $\alpha: \mathcal{X} \to \mathbb{P}_1(\mathbb{k})$ is a separable covering. If (\mathcal{X}, α) is an Abel pair of degree n then there exist $x \in \mathbb{k}[\mathcal{X}]$ with $\deg x = k$, and polynomials $P_1, P_2, \ldots, P_{k-1} \in \mathbb{k}[x]$ with $\deg P_i \leqslant n$, such that the equation of the curve \mathcal{X} can be written as

$$\alpha^{k} + \alpha^{k-1} P_{k-1}(x) + \dots + \alpha P_{1}(x) + x^{n} = 0$$

Proof. Let (\mathcal{X}, α) be an Abel pair. Then $\mathbb{k}(\mathcal{X})/\mathbb{k}(\alpha)$ is a finite extension of fields. By the primitive element theorem there is an element x such that $\mathbb{k}(\mathcal{X}) = \mathbb{k}(\alpha)(x)$. Let $F \in \mathbb{k}[\alpha, t]$ be the minimal polynomial of x, i.e., $\mathbb{k}(\mathcal{X}) = \mathbb{k}(\alpha)[t]/(F)$.

Let $\operatorname{div}(\alpha) = nA - nB$. By using a linear fractional transformation, we may assume that x(A) = 0 and $x(B) = \infty$.

We thus obtain the equation of the curve $F(\alpha, x) = 0$.

We expand F in powers of α : $\alpha^k P_k(x) + \alpha^{k-1} P_{k-1}(x) + \cdots + \alpha P_1(x) + P_0(x)$. By considering the degree of α , we get $\deg P_i \leqslant n$. The condition $\operatorname{div}(\alpha) = nA - nB$ implies that $P_0(x) = x^n$ and $P_k(x) = 1$.

Conversely, from the form of the equation it is clear that α has the divisor nA-nB.

Later in this article we will assume that \mathcal{X} is a hyperelliptic curve. In this case we obtain the following proposition:

Proposition 4.2. Suppose that char $\mathbb{k} \neq 2$.

(i) If (\mathcal{X}, α) is an Abel pair of degree n then there exist $x \in \mathbb{C}[\mathcal{X}]$ with $\deg x = 2$, and a polynomial P with $\deg P \leqslant n$, such that the equation of the curve \mathcal{X} can be written as

$$F(\alpha, x) = \alpha^2 + \alpha P(x) + x^n = 0.$$

- (ii) If the genus of X is 1 then $\deg P \leqslant \frac{n}{2}$, and also in the case of even n the leading coefficient of P is 2.
- (iii) div $\alpha = nA nB$. Then A is a smooth point of \mathcal{X} if and only if $P(0) \neq 0$.
- (iv) Let (x_0, α_0) be a point on \mathcal{X} , with $\alpha_0 \neq 0$. It is a critical point of α if x_0 satisfies the equation

$$n^{2}x_{0}^{n-1} - nP(x_{0})P'(x_{0}) + x_{0}(P'(x_{0}))^{2} = 0.$$

- **Proof.** (i) Let us specify the coordinates (x,y) of \mathcal{X} so that its equation has the form $y^2 = f(x)$ and $x(B) = \infty$, so the Abel function takes the form $\alpha = P(x) + Q(x)y$. Then the equation of \mathcal{X} takes the form $\alpha^2 + 2\alpha P(x) + x^n = 0$.
- (ii) \mathcal{X} is elliptic, $\alpha = P(x) + Q(x)y$ and $\deg \alpha = n$, so $\deg P \leqslant \frac{n}{2}$. For even n we have $P^2/4 x^n = f(x)Q^2(x)$ and $\deg f = 3$, so the degree of $P^2/4 x^n$ is odd, and the leading coefficient of P^2 is 4.
- $P^2/4 x^n$ is odd, and the leading coefficient of P^2 is 4. (iii) $\frac{\partial F}{\partial x} = \alpha + nx^{n-1}$ and $\frac{\partial F}{\partial \alpha} = 2\alpha + P(x)$, x(A) = 0 and $\alpha = 0$, so A is singular if and only if P(0) = 0.
- (iv) α_0 is a critical value of α if and only if $F(x, \alpha_0)$ has a multiple root, i.e., $F(x_0, \alpha_0) = 0$ and $\frac{\partial F(x, \alpha)}{\partial x}\Big|_{(x_0, \alpha_0)} = 0$. But $\frac{\partial F(x, \alpha)}{\partial x}\Big|_{(x_0, \alpha_0)} = \alpha_0 P'(x_0) + nx_0^{n-1} = 0$, i.e., $\alpha_0 = -nx_0^{n-1}/P'(x_0)$, so x_0 is a root of $F(x, -nx^{n-1}/P'(x))$.

Notation 4.3. We introduce the polynomials

$$R_n(x) := -\left(\frac{-1 + \sqrt{1 - 4x}}{2}\right)^n - \left(\frac{-1 - \sqrt{1 - 4x}}{2}\right)^n$$
$$= -2^{1 - \frac{n}{2}} x^{\frac{n}{2}} T_n \left(-\frac{1}{2\sqrt{x}}\right),$$

where T_n is a Chebyshev polynomial. For example $R_0(x) = -2$, $R_1(x) = 1$, $R_2(x) = 2x - 1$, $R_3(x) = -3x + 1$, $R_4(x) = -2x^2 + 4x - 1$, $R_5(x) = 1 - 5x + 5x^2$,...

- **Proposition 4.4.** (i) Let \mathcal{X} be the algebraic curve over \mathbb{k} defined by an equation $\alpha^2 + \alpha P(x) + x^n = 0$ with $\deg P \leqslant n/2$, and suppose that char $\mathbb{k} \nmid n$. The curve \mathcal{X} is rational if and only if $P(x) = C^{2k-n}x^kR_{n-2k}(C^2x)$, where $k \leqslant n/2$ and $C \in \mathbb{k}$.
 - (ii) Let the pair (\mathcal{X}, α) be defined by the equation $\alpha^2 + \alpha x^k R_{n-2k}(x) + x^n = 0$. Then there exists $t \in \mathbb{k}(\mathcal{X})$ such that $\alpha = t^{n-k}(-t-1)^k$.

Proof. (i) Firstly, let $P(0) \neq 0$, so A is a smooth point of \mathcal{X} . In the notation of the preceding proof we obtain $\frac{P^2(x)}{4} - x^n = f(x)Q^2(x)$, and \mathcal{X} is rational if and only if $\deg f \leq 2$. Moreover, from $\deg(\frac{P^2}{4} - x^n) = n$ we get $\deg f = 1$ for odd n and $\deg f = 2$ for even n.

Next we make a change of variables in the identity $\frac{P^2}{4} - x^n = f(x)Q^2(x)$; let $x := 1/t^2$, so that $(t^n \cdot P(1/t^2)/2)^2 = f(1/t^2)Q^2(1/t^2) \cdot t^{2n} + 1$. From this identity we see that $t^n \cdot P(1/t^2)$ is a Shabat polynomial, and we get the valencies of its critical point. Thus we get $t^n \cdot P(1/t^2) = 2T_n(Const \cdot t)$.

Secondly, let us consider the case P(0) = 0. We have $P(x) = x^k P_1(x)$, with $P_1(0) \neq 0$. We reduce this to the previous case by the change of variables $\alpha_1 = \alpha/x^k$.

(ii) We have

$$t = \frac{-1 + \sqrt{1 - 4x}}{2} = -\frac{2\alpha + 2Q + P}{4Q} \in \mathbb{k}(\mathcal{X}).$$

Then t(-t-1) = x and $t^m + (-1-t)^m = R_m(x)$, so $\alpha = x^k t^{n-2k} = t^{n-k} (-t-1)^k$.

§5. Abel pairs of genus 1

5.1. The family of Abel pairs of genus 1. The modular curve $Y_1(n)$ (see [4]) parametrizes the pairs $(\mathcal{E}, A - B)$, where \mathcal{E} is an elliptic curve and A - B is a divisor on it of order exactly n. Let us recall that the order of a divisor is its order as element of Jacobian variety $J(\mathcal{E})$. The modular curve $X_1(n)$ compactifies $Y_1(n)$, i.e., stable curves are added at the punctures of $Y_1(n)$.

An Abel pair of genus 1 is actually determined by an arbitrary elliptic curve and two points A, B such that $n(A-B)\equiv 0$. However, the true order of the divisor (A-B) may be less than n, meaning that such an Abel function is a power of another Abel function.

Next we will see that $X_1(n)$ is the base of a family of Abel pairs.

Definition 5.1. An Abel pair (\mathcal{X}, α) is called imprimitive if there exists another Abel pair (\mathcal{X}, α_0) and a natural number k > 1 such that $\alpha = \alpha_0^k$. Otherwise, the Abel pair is called primitive.

- (i) The parameter space of Abel pairs of genus 1 and degree n has $\sigma_0(n) - 1$ components, where $\sigma_0(n)$ is the number of $divisors \ of \ n.$
 - (ii) Each number d such that $d \mid n$ and 1 < d corresponds to a component of the parameter space of Abel pairs of genus 1 and degree n, consisting of Abel pairs which are the n/d-th powers of primitive Abel pairs of genus 1.
 - (iii) Y(n) is isomorphic to the space of parameters of elliptic primitive Abel pairs.

Proof. See [3], Proposition 3.2.

Theorem 5.3. (i) Besides 0 and ∞ , a generic Abel function α (excluding a finite set of Abel functions) on a curve of genus 1 has exactly two more critical values: $\{k_1, k_2\}$.

(ii) The function

$$\varkappa_n = \frac{2 - \frac{k_1}{k_2} - \frac{k_2}{k_1}}{4} = -\frac{(k_1 - k_2)^2}{4k_1k_2}$$

is a well-defined Belyi function on $X_1(n)$.

Proof. (i) Let e_P be the ramification index of α at the point P. Then by the Riemann–Hurwitz formula we get $2 \deg \alpha = \sum_{P \in \mathcal{X}} (e_P - 1)$. However

$$\operatorname{div}(\alpha) = nA - nB$$
, so $e_A = e_B = n = \operatorname{deg} \alpha$.

 $\operatorname{div}(\alpha) = nA - nB$, so $e_A = e_B = n = \deg \alpha$. Consequently $2 = \sum_{P \in \mathcal{X} \setminus \{A,B\}} (e_P - 1)$. Therefore, we have two possibil-

ities: two points with ramification index 2 (call them C_1 and C_2) or one point with ramification index 3. Thus α has one or two critical values besides 0 and ∞ . The cases with one additional critical value correspond to Abel-Belyi pairs in which we assume that $k_1 = k_2$. The Abel-Belyi pairs with degree n constitute a finite set.

(ii) $\alpha(C_1) = k_1$ and $\alpha(C_2) = k_2$ are defined up to multiplication by a constant, common inversion and permutation, so $\frac{k_1}{k_2} + \frac{k_2}{k_1}$ is a well-defined function on $X_1(n)$, and hence so is \varkappa_n .

Define $\lambda(t)=(2-t-1/t)/4$, so $\varkappa_n=\lambda(k_1/k_2)$. The critical values of the function $\left(2-\frac{k_1}{k_2}-\frac{k_2}{k_1}\right)/4$ are either the critical points of $\lambda(t)$ or the values of λ at the critical values of k_1/k_2 . The critical values of λ are 0, 1 and ∞ . The critical values of k_1/k_2 are 0, 1 and ∞ , because k_1/k_2 is a local parameter at any other point, so \varkappa_n is a Belyi function.

5.2. Abel-Belyi pairs of genus 1.

Proposition 5.4. The dessins on the torus corresponding to Abel–Belyi pairs have sets of valencies $(n|n|3,1,1,\ldots,1)$ or $(n|n|2,2,1,\ldots,1)$.

Proof. For a torus dessin corresponding to an Abel–Belyi pair with the set of valencies $(n|n|a_1,\ldots,a_k)$, we have k=n-2 by the Riemann–Hurwitz formula. Since $a_1+\ldots+a_k=n$, we obtain the desired assertion.

Proposition 5.5. (i) A dessin with a set of valencies $(n|n|3,1,\ldots,1)$ is determined uniquely by a set $\langle a,b,c\rangle$, defined up to a cyclic permutation, where a+b+c=n.

We denote this dessin by $\bigcirc_{a,b,c}$

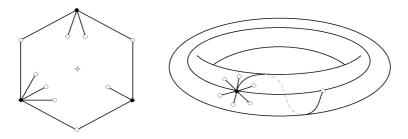
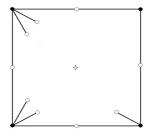


Fig. 1. $\bigcirc_{4,2,3}$.

(ii) A dessin with a set of valencies (n|n|2, 2, ..., 1) is uniquely defined by a set $\langle a, b, c, d \rangle$, defined up to a cyclic permutation, where a+b+c+d=n.

We denote this dessin by $\square_{a,b,c,d}$

Proof. (i) Let us consider a dessin with a set of valencies (n|n|3, 1, ..., 1). This torus dessin has one white vertex of valency 3, and the others have valency 1, i.e., they are terminal vertices. Let us erase the terminal vertices



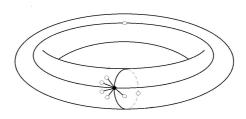


Fig. 2. $\square_{3,2,1,3}$.

and their incident edges, so that the valency list now takes the form (3|3|3). The resulting dessin is unique, consisting of a hexagon with opposite sides identified.

Next we return the previously erased white terminal vertices to this dessin (3|3|3). They can each be added in one of three angles between the three edges emanating from the black vertex of (3|3|3). Let the numbers of vertices placed in these angles, read anticlockwise, be a-1, b-1 and c-1. These numbers define the original dessin $\bigcirc_{a,b,c}$ uniquely.

The case of $\square_{a,b,c,d}$ is treated in a similar way.

Theorem 5.6. (i) A torus dessin $\bigcirc_{a,b,c}$ corresponds to a Belyi function which is an m-th power if and only if m divides gcd(a,b,c).

(ii) A torus dessin $\Box_{a,b,c,d}$ corresponds to a Belyi function which is an m-th power if and only if $a \equiv -b \equiv c \equiv -d \pmod{m}$.

Proof. See Theorem 3 in [2].

Notation 5.7. Let us denote by $m_{\bigcirc}(n, \mathbb{k})$ and $m_{\square}(n, \mathbb{k})$ the numbers of Abel–Belyi pairs over \mathbb{k} with sets of valencies $(n|n|3, 1, \ldots, 1)$ and $(n|n|2, 2, 1, \ldots, 1)$ respectively. Let $\widetilde{m}_{\bigcirc}(n, \mathbb{k})$ and $\widetilde{m}_{\square}(n, \mathbb{k})$ denote the numbers of such primitive pairs.

Recall that we count Abel–Belyi pairs (\mathcal{X}, α) with the weight $1/|\operatorname{Aut}(\mathcal{X}, \alpha)|$.

For instance $m_{\bigcirc}(6,\mathbb{C})=3\frac{1}{3}$. Indeed here is the list of Abel–Belyi pairs over \mathbb{C} with the set of valencies (6|6|3,1,1,1): $\bigcirc_{4,1,1}$, $\bigcirc_{3,2,1}$, $\bigcirc_{3,1,2}$ and $\bigcirc_{2,2,2}$, the last one with an automorphism group of order 3. However $\tilde{m}_{\bigcirc}(6,\mathbb{C})=3$.

Next, $m_{\square}(6,\mathbb{C}) = 2\frac{1}{2}$. The list of Abel–Belyi pairs over \mathbb{C} with the set of valencies (6|6|2,2,1,1) is $\square_{2,2,1,1}$, $\square_{3,1,1,1}$, $\square_{2,1,2,1}$, the last one with an automorphism group of order 2. However $\widetilde{m}_{\square}(6,\mathbb{C}) = 1$, and only $\square_{2,2,1,1}$ is primitive: $\square_{3,1,1,1}$ corresponds to a Belyi function which is a square, and $\square_{2,1,2,1}$ corresponds to a cube.

Theorem 5.8. If n > 3 then

(i)
$$m_{\bigcirc}(n,\mathbb{C}) = \frac{(n-1)(n-2)}{6}, \quad m_{\square}(n,\mathbb{C}) = \frac{(n-1)(n-2)(n-3)}{24};$$

(ii) $m_{\bigcirc}(n,\mathbb{C}) = \sum_{1 \leq d,d \mid n}^{6} \widetilde{m}_{\bigcirc}(d,\mathbb{C});$

(iii)
$$\widetilde{m}_{\mathbb{O}}(n,\mathbb{C}) = \frac{\varphi(n)\psi(n)}{6} - \frac{\varphi(n)}{2}$$
, $\widetilde{m}_{\mathbb{D}}(n,\mathbb{C}) = \frac{(n-6)\varphi(n)\psi(n)}{24} + \frac{\varphi(n)}{2}$, where φ is the Euler function and ψ is the Dedekind psi function $\psi(n) = n \prod_{n|n} \left(1 + \frac{1}{p}\right)$.

Proof. (i) The number of $\bigcirc_{a,b,c}$ is the number of solutions of the equation a+b+c=n in positive integers, divided by 3 (because of rotations of the hexagon), so $m_{\bigcirc}(n,\mathbb{C})=\binom{n-1}{2}/3$. Similarly, $m_{\square}(n,\mathbb{C})=\binom{n-1}{3}/4$.

(ii) According to Theorem 5.6, an Abel–Belyi pair $\bigcirc_{a,b,c}$ is primitive if and only if $\gcd(a,b,c)=1$. Also, for all a,b,c,k we have $\alpha_{\bigcirc ka,kb,kc}=\alpha_{\bigcirc a,b,c}^k$. Every Abel–Belyi function $\alpha_{\bigcirc a,b,c}$ is a power of a primitive Abel–Belyi function, so the number $m_{\bigcirc}(n,\mathbb{C})$ of all pairs is the sum of the numbers of primitive pairs with degree $d\mid n$, i.e., $\widetilde{m}_{\bigcirc}(d,\mathbb{C})$.

(iii) Apply the Möbius inversion formula $\widetilde{m}_{\bigcirc}(n,\mathbb{C}) = \sum_{d|n} m_{\bigcirc}(d)\mu(n/d)$

to (ii). By using (i) we get

$$\widetilde{m}_{\bigcirc}(n,\mathbb{C}) = \sum_{d \mid n} \frac{(d-1)(d-2)}{6} \mu\left(\frac{n}{d}\right) = \frac{\varphi(n)\psi(n)}{6} - \frac{\varphi(n)}{2}.$$

The formula for $\widetilde{m}_{\square}(n,\mathbb{C})$ is proved in the same way by more cumbersome considerations.

5.3. The dessin on $X_1(n)$ **corresponding to** \varkappa_n . In the next proposition we classify the critical points of \varkappa_n .

Theorem 5.9. Let char $\mathbb{k} \neq 2, 3$, and char $\mathbb{k} \nmid n$. The critical points of \varkappa_n on $Y_1(n)$ belong to one of the following three types:

- (i) Each primitive Abel-Belyi pair of type $\bigcirc_{a,b,c}$ corresponds to a zero of multiplicity 3 of \varkappa_n ;
- (ii) Each primitive Abel-Belyi pair of type $\square_{a,b,c}$ corresponds to a zero of multiplicity 2 of \varkappa_n ;
- (iii) Other critical points of \varkappa_n correspond to the critical value $\varkappa_n = 1$ and have multiplicity 2.

Proof. Recall that

$$\varkappa_n = \frac{2 - \frac{k_1}{k_2} - \frac{k_2}{k_1}}{4} = -\frac{(k_1 - k_2)^2}{4k_1k_2}.$$

The function $1/4k_1k_2$ has no zeros or poles on $Y_1(n)$ so the zeros of \varkappa_n are those of $(k_1 - k_2)^2$. This function has its zeros on $Y_1(n)$ where $k_1 = k_2$, i.e., in the case of Abel–Belyi pairs.

Now we consider primitive pairs $\bigcirc_{a,b,c}$ and $\square_{a,b,c}$. In the notation of Theorem 5.3 $(k_1 - k_2)^2 = (\alpha(C_1) - \alpha(C_2))^2$.

In the case $\Box_{a,b,c,d}$ the critical points C_1 and C_2 are different. Locally $\alpha(C_1)$ and $\alpha(C_2)$ are well-defined functions on the base and $\alpha(C_1) - \alpha(C_2)$ has a simple zero because it is a local parameter (char $\mathbb{k} \neq 2,3$). Thus \varkappa_n has a zero of multiplicity 2 at $\Box_{a,b,c,d}$.

In the case $\bigcirc_{a,b,c}$ the critical points C_1 and C_2 coincide. Then the functions $(\alpha(C_1) - \alpha(C_2))/(x(C_1) - x(C_2))$ and $x(C_1) - x(C_2)$ are local parameters on the base and have a simple zero at $\bigcirc_{a,b,c} \in X_1(n)$, so \varkappa_n has a zero of multiplicity 3 at $\bigcirc_{a,b,c}$.

By Theorem 5.3 the other critical points of \varkappa_n correspond to the case $\varkappa_n = 1$. At such a point $k_1 = -k_2$ and k_1/k_2 is a local parameter, so \varkappa_n has multiplicity 2.

Corollary 5.10. Let \bigcirc_1^n , \bigcirc_2^n ,... be the list of primitive Abel–Belyi pairs with sets of valencies $(n|n|3,1,1,\ldots,1)$, and let \square_1^n , \square_2^n ,... be the list of primitive Abel–Belyi pairs with sets of valencies $(n|n|2,2,1,\ldots,1)$. Then

$$\operatorname{div}(\boldsymbol{\varkappa}_n) = 3 \cdot (\boldsymbol{\uprightarrow}_1^n + \boldsymbol{\uprightarrow}_2^n + \ldots) + 2(\boldsymbol{\uprightarrow}_1^n + \boldsymbol{\uprightarrow}_2^n + \ldots) + (points from X_1(n) \setminus Y_1(n))$$

Theorem 5.11. Let char $\mathbb{k} \neq 2, 3$, char $\mathbb{k} \nmid n$. Any point of $X_1(n) \setminus Y_1(n)$ belongs to one of the following types.

(i) Points whose Abel-Belyi pairs have representatives $\alpha^2 + \alpha R_n(x) + x^n = 0$. There are $\varphi(n)/2$ such points in $X_1(n) \setminus Y_1(n)$. At these points \varkappa_n has simple zeros.

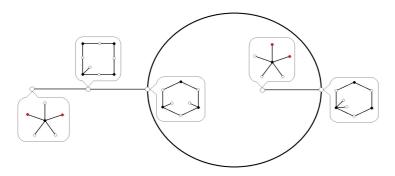


Fig. 3. Dessin on $X_1(5)$ corresponding to \varkappa_5 .

- (ii) Points whose Abel-Belyi pairs have representatives $\alpha^2 + \alpha x^k R_{n-2k}(x) + x^n = 0$, where k satisfies the following conditions: $0 < k < \frac{n}{2}$, $\operatorname{char} \mathbb{k} \nmid k$, $\operatorname{char} \mathbb{k} \nmid (n-k)$. There are $\varphi(\gcd(n,k))$ such points in $X_1(n) \setminus Y_1(n)$. At these points \varkappa_n has poles of multiplicity $k(n-k)/\gcd(n,k)$.
- (iii) Points whose Abel-Belyi pairs have representatives $\alpha^2 + 2\alpha x^{n/2} + x^n = 0$. This case is possible only for even n, in which case there are $\varphi(n/2)/2$ such points in $X_1(n) \setminus Y_1(n)$. At these points \varkappa_n has poles of multiplicity n/2.
- (iv) Points whose Abel-Belyi pairs have representatives $\alpha^2 + \alpha x^k R_{n-2k}(x) + x^n = 0$, where char k > 0 and k satisfies the conditions 0 < k < n, char $k \mid k$. There are $\varphi(\gcd(n,k))$ such points in $X_1(n) \setminus Y_1(n)$. At these points $\varkappa_n = 1$ if k is odd, and $\varkappa_n = 0$ if k is even. The multiplicity of \varkappa_n at these critical points is $k(n-k)/p^{\operatorname{ord}_p(k)} \cdot \gcd(n,k)$.

Proof. In case (i) the Abel pair, in the notation of Theorem 5.3, corresponds to $k_1 = k_2 = 1$ and $C_1 = C_2$, but this point is singular (a double point). By Proposition 4.4(ii), after resolution of the singularity this Abel pair takes the form $(\mathbb{P}^1(\mathbb{k}), t^n)$; in this form the double point has two preimages, at which t takes values belonging to $\sqrt[n]{1}$. To count such pairs we should choose two different points with $t \in \sqrt[n]{1}$ as the normalization of preimages of C. Due to the rotations we have n/2 Abel pairs. Excluding Abel pairs that lie over $X_1(d)$ where $d \mid n, d < n$, we have $\varphi(n)/2$ pairs.

(ii)-(iii) In these cases we have a pole of \varkappa_n on $X_1(n)\setminus Y_1(n)$, i.e., $k_1k_2=0$.

By Proposition 4.4(ii), $\alpha = t^{n-k}(-t-1)^k$. To calculate the multiplicity of this pole let us consider the locally critical value k_1 approaching zero. We define $x_1 = x(C_1)$. Locally at t = 0 and t = -1, α has the form At^k or $B(t+1)^{n-k}$ for some $A, B \in \mathbb{k}$. By changing variables back to x we get $k_1 = Ax_1^{1/k} = Bx_1^{1/(n-k)}$. This equation has $k(n-k)/\gcd(n,k)$ solutions for x_1 , since char $\mathbb{k} \nmid k$ and char $\mathbb{k} \nmid (n-k)$, so the multiplicity of this pole of \varkappa_n is also $k(n-k)/\gcd(n,k)$. The calculation of the number of such poles is the same as in case (i).

(iv) In this case let both k_1 and k_2 go to 0. We want to calculate the indeterminate form k_1/k_2 . We define $x_1 = x(C_1)$, $x_2 = x(C_2)$. Locally we have $x_1 = -x_2$, so $k_2/k_1 = (-1)^k$, i.e., at these points $\varkappa_n = 1$ if k is odd, and $\varkappa_n = 0$ if k is even. Calculating the multiplicity and the number of such points is the same as in cases (i) and (ii).

Proposition 5.12. deg $\varkappa_n = n\varphi(n)\phi(n)/12$.

Proof. From the preceding theorem,

$$\deg \varkappa_n = \frac{1}{2} \sum_{k=1}^{n-1} \frac{\varphi(\gcd(n,k))}{\gcd(n,k)} k(n-k) = \frac{n\varphi(n)\psi(n)}{12}.$$

To calculate the numbers m_{\square} and m_{\bigcirc} we need also to take into account the imprimitive Abel pairs. We therefore consider all the components of bases of families of Abel pairs, i.e., the curves $X_1(d)$ for $1 < d, \ d \mid n$. The function $(2 - \frac{k_1}{k_2} - \frac{k_2}{k_1})/4$ is a well-defined Belyi function on each of these components. We denote it by $\varkappa_{d,n}$.

Proposition 5.13. If d > 1 is a divisor of n, then $\varkappa_{d,n} = (T_{n/d} \circ \varkappa_d + 1)/2$.

Proof. By Theorem 5.2

$$\varkappa_{d,n} = \frac{2 - \frac{k_1}{k_2} - \frac{k_2}{k_1}}{4} = \frac{2 - \frac{\kappa_1^{n/d}}{\kappa_2^{n/d}} - \frac{\kappa_2^{n/d}}{\kappa_1^{n/d}}}{4} = \frac{T_{n/d}(\varkappa_d) + 1}{2}.$$

where κ_1 and κ_2 are the critical points of an imprimitive Abel pair of genus 1 and degree n/d.

§6. The number of Abel-Belyi pairs of genus 1

Excluding statements concerning the lists of Abel–Belyi pairs of genus 1, obtained by topological arguments, all the above statements are valid in the case of positive characteristic (under the conditions char $\mathbb{k} \nmid n$, char $\mathbb{k} \neq 2,3$).

We now find the number of Abel–Belyi pairs of genus 1 in positive characteristic. Instead of topological considerations, which not available now, we use algebraic arguments, especially the study of the divisor of \varkappa_n . We will use results 5.9-5.13.

Proposition 6.1.

(i)
$$2m_{\square}(n,\mathbb{C}) + 3m_{\bigcirc}(n,\mathbb{C}) = (n-1)(n-2)(n+3)/12$$
.

(ii)
$$\deg \varkappa_n(\mathbb{C}) - \deg \varkappa_n(\overline{\mathbb{F}_p}) = \sum_{k=1}^{\lfloor n/p \rfloor} \frac{\varphi(\gcd(k,n))}{\gcd(k,n)} kp(n-kp).$$

(iii)
$$2m_{\square}(n,\mathbb{C}) + 3m_{\bigcirc}(n,\mathbb{C}) - 2m_{\square}(n,\overline{\mathbb{F}_p}) - 3m_{\bigcirc}(n,\overline{\mathbb{F}_p})$$

$$= \sum_{k=1}^{\lfloor n/p \rfloor} kp(n-kp) + \sum_{k=1}^{\lfloor n/2p \rfloor} \frac{2k}{p^{\operatorname{ord}_p(k)}}(n-2kp).$$

Proof. For (i) use Proposition 5.13:

$$\sum_{1 < d \mid n} \deg \varkappa_{d,n} = \sum_{1 < d \mid n} \frac{n}{d} \deg \varkappa_d = n \sum_{1 < d \mid n} \frac{\varphi(d) \psi(d)}{12} = \frac{n(n-1)(n+1)}{12}.$$

By results 5.9-5.11 the function $\varkappa_{d,n}$ has $\varphi(d)/2$ simple zeros, described in Theorem 5.11(i), besides the points of $X_1(d)$ over which Abel–Belyi pairs of genus 1 lie. By summing the numbers of all the simple zeros of the functions $\varkappa_{d,n}$, we have $\sum_{1 < d, \, d|n} \varphi(d)/2 = (n-1)/2$ simple zeros, so from

Corollary 5.10 we get

$$2m_{\square}(n) + 3m_{\bigcirc}(n) = \frac{n(n-1)(n+1)}{12} - \frac{n-1}{2} = \frac{(n-1)(n-2)(n+3)}{12}.$$

For (ii) we calculate the difference between the degrees of $\varkappa_n(\mathbb{C})$ and $\varkappa_n(\overline{\mathbb{F}_p})$. Let us compare the list of poles of \varkappa_n over \mathbb{C} and $\overline{\mathbb{F}_p}$. By Theorem 5.11(iii), in the case of $\overline{\mathbb{F}_p}$ the poles of \varkappa_n of degree $kp(n-kp)/\gcd(k,n)$ with 0 < k < n/p disappear.

For (iii), by Theorem 5.11(iv) in characteristic char $\mathbb{k} = p$ the list of zeros of $\varkappa_n(\overline{\mathbb{F}_p})$, as compared with the case of char $\mathbb{k} = 0$, has additional zeros on $X_1(n) \setminus Y_1(n)$. The list of its multiplicities is $2k(n-2kp)/p^{\operatorname{ord}_p(k)} \gcd(n,k)$, where 0 < k < n/2p. By summing these multiplicities of zeros for $\varkappa_{d,n}(\overline{\mathbb{F}_p})$

where $1 < d, d \mid n$, and by (ii), we calculate the difference between the numbers of zeros of $\varkappa_n(\mathbb{C})$ and $\varkappa_n(\overline{\mathbb{F}_p})$ on $Y_1(n)$. By Theorem 5.9 this is $2m_{\square}(n,\mathbb{C}) + 3m_{\bigcirc}(n,\mathbb{C}) - 2m_{\square}(n,\overline{\mathbb{F}_p}) - 3m_{\bigcirc}(n,\overline{\mathbb{F}_p})$.

The previous theorem is insufficient to calculate $m_{\square}(n, \overline{\mathbb{F}_p})$ and $m_{\bigcirc}(n, \overline{\mathbb{F}_p})$. To calculate these quantities separately, we need one more equation. We will use the genus of $X_1(n)$.

Lemma 6.2.

$$genus(X_1(n, \overline{\mathbb{F}_p})) = genus(X_1(n)) = \frac{\varphi(n)\psi(n)}{24} - \frac{\varphi(n)\sigma_0(n)}{4} + 1.$$

Proof. For char k = 0 we can apply Theorems 5.8, 5.9, 5.11(i)–(iii) and the Riemann–Hurwitz formula to the function \varkappa_n on $X_1(n)$. By Igusa's theorem for $p \nmid n$ the curve $X_1(n)$ has good reduction at p. See 8.6.1 in [4].

Theorem 6.3. (i)
$$m_{\square}(n,\mathbb{C}) - m_{\square}(n,\overline{\mathbb{F}_p}) = \sum_{0 < k < n/p} (n-kp).$$
 (ii) $m_{\square}(n,\mathbb{C}) - m_{\square}(n,\overline{\mathbb{F}_p}) = \sum_{k=1}^{\lfloor n/p \rfloor} \frac{kp-3}{2} (n-kp) + \sum_{k=1}^{\lfloor n/2p \rfloor} \frac{k}{p^{\operatorname{ord}_p(k)}} (n-2kp).$

Proof. We apply the Riemann–Hurwitz formula to $\varkappa_n(\mathbb{C})$ and $\varkappa_n(\overline{\mathbb{F}_p})$ to calculate $genus(X_1(n,\overline{\mathbb{F}_p}))$ and $genus(X_1(n))$. From the preceding lemma $genus(X_1(n,\overline{\mathbb{F}_p})) = genus(X_1(n,\mathbb{C}))$, so we consider the difference between these two formulae. We also sum these differences over all the divisors of n (as in proof of 6.1(iii)), and we get $2(m_{\bigcirc}(n) - m_{\bigcirc}(n,\overline{\mathbb{F}_p})) + (m_{\square}(n) - m_{\square}(n,\overline{\mathbb{F}_p})) = \frac{p+1}{2}(n-p) + (p+1)(n-2p) + \frac{3p+1}{2}(n-3p) + 2(p+1)(n-4p) + \dots$

By 6.1(iii) we get (ii) and

$$m_{\bigcirc}(n,\overline{\mathbb{F}_p}) = m_{\bigcirc}(n,\mathbb{C}) - (n-p) - (n-2p) - \dots$$

Remark 6.4. Note that in the case p > n we have $m_{\square}(n, \overline{\mathbb{F}_p}) = m_{\square}(n, \mathbb{C})$ and $m_{\bigcirc}(n, \overline{\mathbb{F}_p}) = m_{\bigcirc}(n, \mathbb{C})$.

§7. Example

7.1. Method: Padé approximation. We describe our method for calculating the Abel pairs of genus 1:

Definition 7.1. The Padé approximant (see [5]) of order [n,m] of a real-valued function $f(x) \in C^{n+m}(U)$, where $U \subset \mathbb{R}$ is a neighborhood of 0, is the ratio of two polynomials $R_{[n,m]} = \frac{p_{[n,m]}(x)}{q_{[n,m]}(x)}$, with $\deg p_{[n,m]}(x) \leqslant m$ and $\deg q_{[n,m]}(x) \leqslant n$, for which $f^{(i)}(0) = R_{[n,m]}^{(i)}(0)$ for $0 \leqslant i \leqslant m+n$.

Let \mathcal{E} be an elliptic curve. We want to find $\alpha \in \mathbb{k}(\mathcal{E})$ such that $\operatorname{div}(\alpha) = nA - nB$. Let \mathcal{E} be defined by the equation $y^2 = 1 + ax + bx^2 + cx^3$, such that x(A) = 0, y(A) = 1 and B is the infinite point.

Theorem 7.2. Let the rational function p(x)/q(x) be the Padé approximant of the function $\sqrt{1+ax+bx^2+cx^3}$ of order $[\lfloor n/2 \rfloor, \lfloor (n-3)/2 \rfloor]$. Then for the function $\mathfrak{a}=p(x)-q(x)y$ on $\mathcal E$ we have $\operatorname{div}(\mathfrak{a})=(n-1)A+C-B$, where C is some point on $\mathcal E$.

Proof. See
$$[7]$$
.

The Padé approximants of the function f(x) are determined by the Taylor coefficients of f(x) which are functions depending on a, b, c. The condition A = C means that one more Taylor coefficient of f(x) and p(x)/q(x) are equal. This gives us the algebraic equation on a, b, c.

7.2. The case n = 6. After a series of calculations we get an equation for the family of primitive Abel pairs of degree 6 parametrized by a variable t (i.e., $X_1(6)$ is rational):

$$\alpha^{2} + \left(-t(t-1)^{2} - (3t+1)(t-1)x - 4x^{2} + 2x^{3}\right)\alpha + x^{6} = 0,$$

$$\varkappa_{6}(\mathbb{C}) = -\frac{1}{2^{14} \cdot 3^{12}} \frac{(9 t - 1) (81 t^{3} - 27 t^{2} + 99 t - 25)^{3} (9 t - 25)^{2}}{t^{5} (t - 1)^{4}}.$$

Let us see what the zeros and poles of \varkappa_6 are.

The poles of \varkappa_6 are located at the points t=0, t=1 and $t=\infty$. For t=0 the equation takes the form $\alpha^2 - xR_4(x)\alpha + x^6 = 0$. At t=1 we have $\alpha^2 + 4x^2R_2(x/4)\alpha + x^6 = 0$, and at $t=\infty$ we have $\alpha^2 + 2x^3\alpha + x^6 = 0$.

The zeros of \varkappa_6 are located at $t=1/9,\ t=25/9$ and at the roots of the equation $81\ t^3-27\ t^2+99\ t-25=0$. At t=1/9 we get the equation $\alpha^2+\frac{2^6}{3^6}R_6(\frac{9}{4}x)\alpha+x^6=0$. At t=25/9 we get the Abel–Belyi pair $\square_{1,1,2,2}$, while the Abel–Belyi pairs $\bigcirc_{4,1,1},\bigcirc_{3,2,1}$ and $\bigcirc_{3,1,2}$ lie at the roots of $81\ t^3-27\ t^2+99\ t-25=0$.

We consider the reduction of this family of curves for characteristic 5. Let us look at the zeros and poles of \varkappa_6 . The zero of \varkappa_6 at t=25/9 now moves to t=0, as does one of the roots of the equation $81 t^3 - 27 t^2 + 99 t - 25 = 0$. In the numerator of \varkappa_6 we have $t^5 \cdot (t^2 + 3t + 4)^3 \cdot (t+1)$, so the pole at t=0 disappears:

$$\varkappa_6(\overline{\mathbb{F}_5}) = -\frac{(t^2 + 3t + 4)^3 \cdot (t+1)}{(t-1)^4}$$

From this calculation we see that over $\overline{\mathbb{F}_5}$ there are only two primitive Abel–Belyi pairs with the set of valencies $(n|3,1,\ldots,1)$, unlike over \mathbb{C} , where exist three such pairs. Also over $\overline{\mathbb{F}_5}$ there are no primitive Abel–Belyi pairs whose set of valencies is $(n|2,2,1\ldots,1)$, unlike over \mathbb{C} where one such pair exists.

Thus $m_{\bigcirc}(6,\mathbb{C}) - m_{\bigcirc}(6,\overline{\mathbb{F}_5}) = 1$ and $m_{\square}(6,\mathbb{C}) - m_{\square}(6,\overline{\mathbb{F}_5}) = 1$, in accordance with Theorem 6.3.

References

- 1. N. H. Abel, Uber die Integration der Differential-Formel $\rho dx/\sqrt{R}$, wenn R und ρ ganze Funktionen sind. J. für Math. 1 (1826), 185–221.
- F. Pakovich, Combinatoire des arbres planaires et arithmétique des courbes hyperelliptiques. — Annales de l'Institut Fourier Volume: 48, Issue: 2, (1998) page 323-351, ISSN: 0373-0956
- 3. D. Chen, I. Coskun, Extremal effective divisors on the $\mathcal{M}_{1,n}$. Mathematische Annalen 359, No. 3 (2014), 891–908.
- F. Diamond, J. Shurman, A First Course in Modular Forms, Springer Science & Business Media (2006).
- G. A. Baker, P. R. Graves-Morris, Padé Approximants, Cambridge Univ. Press, Cambridge (1996). Перевод: Дж. Бейкер, П. Грейвс-Моррис, Annpoксимации Паде. М., Мир. 1986.
- 6. S. Lando, A. Zvonkin, *Graphs on Surfaces and Their Applications*, Encyclopaedia of Mathematical Sciences: Lower-Dimensional Topology II 141, Berlin, New York, (2004). Перевод: А. К. Звонкин, С. К. Ландо, *Графы на поверхностях и их приложения*, М., Изд-во МЦНМО, 2010.
- 7. Д. А. Оганесян, О рациональных функциях с двумя критическими точками максимальной кратности. Фунд. прикл. матем. 18, No. 6 (2013), 185-208. English translation: D. A. Oganesyan, Rational functions with two critical points of maximum multiplicity. J. Math. Sci. (N. Y.) 209, no. 2, 292-308.

Moscow Lomonosov State University

Поступило 30 апреля 2016 г.

E-mail: grag.oganes@gmail.com