An invariant of certain fields of genus 2

H. Borges Neto(*)

0. Introduction and Notations.

The aim of this paper is to describe the isomorphy classes of algebraic functions fields of genus 2 and of absolute genus 1 by using suitable invariants. Using Proposition 2 it is easy to give examples of non isomorphic fields of the kind.

A field K of algebraic functions of one variable over k is said to have genus 2 if and only if there exist $x, y \in K \backslash k$ such that $K = k(x, y)$, $y^2 = f(x) \in k[x]$ has degree 5 or 6 and has no multiple factors over k. In this case, the rational field is characterized as the unique quadratic subfield of K which contains k and has genus 0 (see Artin [1]).

Denote the algebraic closure of k by $\bar{k}$. We say that $K|k$ has absolute genus 1 (or that it is absolutely elliptic) if the composite $K \cdot \bar{k}$ has genus 1 (for genus change see [2], [4] or [5]).

It is easy to see that for $K|k$ with genus 2 to be absolutely elliptic it is necessary and sufficient that char $(k) = 3$ and $K = k(x, y)$, with $y^2 = (x^3 - \alpha)\ (f_0 x^3 + f_1 x^2 + f_2 x + f_3)$, $\alpha \in k \backslash k^3$, and discriminant of $f_0 x^3 + \ldots + f_3$ is non-zero (this last condition is equivalent to $f_1^2 f_2^2 - f_0 f_2^3 - f_3 f_1^3 \neq 0$) (See Borges Neto [3]).

Obviously, $k(\sqrt[3]{\alpha})$ is determined uniquely as it is the smallest extension of k among those that have their composition with K of genus 1.

1. The invariant.

Theorem 1. *Let $K = k(x, y)$ and $K' = k(x, v)$ be two abolutely elliptic fields of genus 2 with $y^2 = f(x) = (x^3 - \alpha)\ (f_0 x^3 + \ldots + f_3)$ and $v^2 = (x^3 - \alpha')$ $(g_0 x^3 + \ldots + g_3)$.*

K and K' are k-isomorphic iff there exists a fractional linear transformation $\psi : \bar{k} \cup \{\infty\}$ given by $z \mapsto \dfrac{az+b}{cz+d}$, if $z \neq \infty$, $\infty \mapsto a/c$ if $c \neq 0$ or ∞ if $c = 0$, where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k)$, such that:

(*) During this work the author held a fellowship by CNPq-Brazil.

Recebido em 22/1/81. Versão definitiva em 12/2/82.

1) $\sqrt[3]{\alpha'} = \psi(\sqrt[3]{\alpha})$;
2) ψ *transforms separable roots of f into those of g;*
3) *if* $f_0 \neq 0$, $\frac{1}{f_0} g(\psi(\infty)) \in k^2 \backslash \{0\}$ *if* $\psi(\infty) \in k$ *and*

$\frac{g_0}{f_0} \in k^2 \backslash \{0\}$ *if* $\psi(\infty) = \infty$.

If $f_0 = g_0 = 0$, $\psi(\infty) = \infty$ *and* $a \in k^2 \backslash \{0\}$.

Proof. ($\leftarrow$) If $\psi(\infty) \in k$ and $f_0 \neq 0$ we consider the k-isomorphism given by $x \mapsto \psi(x)$ and $v \mapsto \sqrt{\frac{g(\psi(\infty))}{f_0}} \frac{1}{(cx+d)^3} y$; if $\psi(\infty) = \infty$ and $f_0 \neq 0$, we consider $x \mapsto \psi(x)$ and $v \mapsto a^3 \sqrt{\frac{g_0}{f_0}} y$. Finally, if $f_0 = 0$ consider $x \mapsto \sqrt{a}\, x + b$ and $v \mapsto \sqrt{a^5}\, y$.

($\mapsto$) Let $\sigma : K' \mapsto K$ be a k-isomorphism. Then $k(x)$ is left invariant by σ as it is the unique subfield of K which contains k and has genus 0. It means that $\sigma|_{k(x)} \in \mathrm{Aut}(k(x)|k)$ and therefore one finds $\{a, b, c, d\} \subset k$ with $ad\text{-}bc \neq 0$ such that $\sigma(x) = \frac{ax+b}{cx+d}$.

As for $\sigma(v)$ we may say that $\sigma(v) = t + uy$, where $t, u \in k(x)$ are uniquely determined and $u \neq 0$.

But $t^2 - tuy + u^2 f(x) = \sigma(v)^2 = g(\sigma(x))$.

Therefore $t = 0$ and $\sigma(v) = uy$. We put $u = r/s$, $r, s \in k[x]$ relatively prime, r monic.

Consequently, as $g(\sigma(v)) = \sigma(v)^2 = \left(\frac{r}{s}\right)^2 f(x)$ we have

$$s^2 \left(\frac{ax+b}{cx+d} - \sqrt[3]{\alpha'}\right)^3 \left[g_0 \left(\frac{ax+b}{cx+d}\right)^3 + \ldots + g_3\right] = r^2(x - \sqrt[3]{\alpha}).$$
$$(f_0 x^3 + \ldots + f_3).$$

Eliminating denominators we obtain

$$(1) \qquad (a - c\sqrt[3]{\alpha'})\, s^2 \left(x - \frac{d\sqrt[3]{\alpha'} - b}{a - c\sqrt[3]{\alpha'}}\right)^3 .$$
$$[(\partial g - 5)\ (g_0 a^3 + g_1 a^2 c + g_2 a c^2 + g_3 c^3) x^3 + \ldots] =$$
$$= (cx+d)^{\partial g}\ r^2 (x - \sqrt[3]{\alpha})^3\ (f_0 x^3 + \ldots + f_3).$$

One easily concludes from equation (1) above that $s = 1$, as otherwise one would have $s^2 = (x - \sqrt[3]{\alpha})^3$, impossible in virtue of degree arguments.

For the same reason r does not divide $\left(x - \frac{d\sqrt[3]{\alpha'} - b}{a - c\sqrt[3]{\alpha'}}\right)^3$. Thus, we infer that

$$(2) \qquad x - \sqrt[3]{\alpha} = x - \frac{d\sqrt[3]{\alpha'} - b}{a - c\sqrt[3]{\alpha'}}.$$

From here we get a fractional k-linear transformation $\psi : k \cup \{\infty\} \mapsto \bar{k} \cup \{\infty\} : z \mapsto \frac{az+b}{cz+d}$ which satisfies

1) $\sqrt[3]{\alpha'} = \frac{a\sqrt[3]{\alpha} + b}{c\sqrt[3]{\alpha} + d}$ (by (2)).

2) ψ sends separable roots of f into those of g (by (1) and (2)).

3) If $f_0 \neq 0$, $\frac{1}{f_0} g(\psi(\infty)) \in k^2 \backslash \{0\}$ if $\psi(\infty) \in k$ or

$\frac{g_0}{f_0} \in k^2 \backslash \{0\}$ if $\psi(\infty) = \infty$.

If $f_0 = 0$, we have $c = 0$, $d = 1$ and $r = \sqrt{a^5}$.

Corollary 1. *Aut*$(K|k) \simeq Z/2Z$.

Corollary 2. *The field* k_0 *of roots of separable factor of f as well as* $k(\sqrt[3]{\alpha})$ *are canonically determined by the class of k-isomorphy of K*.

From now on, we shall suppose that $[k_0 : k] = 2$.

Let $x_0 \in k$ be a root of $f_0 x^3 + \ldots + f_3$. Substituting x by $\dot{x} := \frac{1}{x - x_0}$ and y by $y := \frac{1}{x^3} y$ we may suppose that the polynomial equation which involves generators of $K|k$ has degree 5 and is monic in the variable x.

In those conditions, $w\ell g$, we take the absolutely elliptic fields of genus 2 having generators related by the following condition: $Y^2 = (X^3 - \alpha)(X^2 + f_2 X + f_3)$. $\alpha \in k \backslash k^3$ and $f_2^2 - f_3 \neq 0$.

Proposition 2. *Let* $K = k(x, y)$ *and* $K' = k(x, v)$ *be two absolutely elliptic fields of genus 2, satisfying* $y^2 = (x^3 - \alpha)(x^2 + f_2 x + f_3)$ *and* $v^2 = (x^3 - \alpha')$. $(x^2 + g_2 x + g_3)$.

K and K' are k-isomorphic iff $\frac{f_2 - \sqrt[3]{\alpha}}{g_2 - \sqrt[3]{\alpha'}} \in k^2 \backslash \{0\}$ *and*

$$\frac{(f_2 - \sqrt[3]{\alpha})^2}{f_2^2 - f_3} = \frac{(g_2 - \sqrt[3]{\alpha})^2}{g_2^2 - g_3}.$$

In particular, $\dfrac{(f_2 - \sqrt[3]{\alpha})^2}{f_2^2 - f_3}$ *is an invariant of k-isomorphy class of K.*

Proof. It follows immediately from Theorem 1 that if K and K' are k-isomorphic then an isomorphism is determined by the formulae $x \mapsto a^2x + b$ and $v \mapsto a^5y$.

Applying the isomorphism to the equation $v^2 = g(x)$ we obtain $a^{10}y = (a^2x + b - \sqrt[3]{\alpha'})^3\ (a^4x^2 + a^2(g_2 - b)x + b^2 + g_2b + g_3)$.

But $y^2 = f(x)$, so we arrive at

$$(x - \sqrt[3]{\alpha})^3\ (x^2 + f_2x + f_3) = \left(x - \frac{\sqrt[3]{\alpha'} - b}{a^2}\right)^3 \left(x^2 + \frac{g_2 - b}{a^2}x + \frac{b^2 + g_2b + g_3}{a^4}\right).$$

As $(x - \sqrt[3]{\alpha})^3$ is purely inseparable over k and $x^2 + f_2x + f_3$ is separable, we have $\sqrt[3]{\alpha} = b + a^2\sqrt[3]{\alpha}$, $a^2f_2 = g_2 - b$ and $a^4f_3 = b^2 + g_2b + g_3$.

Thus, K and K' are k-isomorphic iff there exists $a \in k\backslash\{0\}$ such that $\sqrt[3]{\alpha'} - g_2 = a^2(\sqrt[3]{\alpha} - f_2)$ and $a^4(f_2^2 - f_3) = g_2^2 - g_3$.

But on the other hand this is also equivalent to saying that

$$\frac{f_2 - \sqrt[3]{\alpha}}{g_2 - \sqrt[3]{\alpha'}} \in k^2\backslash\{0\} \quad \text{and} \quad \frac{(f_2\sqrt[3]{\alpha})^2}{f_2^2 - f_3} = \frac{(g_2 - \sqrt[3]{\alpha'})^2}{g_2^2 - g_3}.$$

Corollary 3. *Let k be quadratically closed. The fields K and K′ are k-isomorphic iff their invariants coincide.*

References

[1] A. Artin; *Algebraic Numbers and Algebraic Functions*, Gordon and Breach (1967).

[2] H. Borges Neto; *Mudança de Gênero e Classificação de Corpos de Gênero* 2, Tese de Doutoramento, IMPA, Rio de Janeiro, Brasil (1979).

[3] H. Borges Neto; *Absolutely Elliptic Fields of Genus* 2 *and their Normal Form* (to appear).

[4] H. Stichtenoth; *Algebraische Funktionenkörper einer Variablen*, Vorlesungen der Universität Essen (1978).

[5] J. Tate; *Genus Change in Inseparable Extension Fields*, Proc. Amer. Math. Soc. 3 (1952), 400-406.

Departamento de Matemática – UFC
60.000 – Fortaleza – CE
Brasil