Arch. Math. 101 (2013), 599–600
© 2013 Springer Basel
0003-889X/13/060599-2
published online November 28, 2013
DOI 10.1007/s00013-013-0582-4

Archiv der Mathematik

ERRATUM

Erratum to: Fields of moduli and definition of hyperelliptic covers

Yolanda Fuertes and Gabino González-Diez

Mathematics Subject Classification (2000). 14H37, 14H45, 14G99.

Keywords. Hyperelliptic curves, Automorphisms, Field of moduli, Field of definition.

Erratum to: Arch Math 86 (2006) 398–408
DOI 10.1007/s00013-005-1433-8

Consider the algebraic curve

$$C:\ y^2=\prod_{d=4}^{2g+2}\left(x^4-2\left(1-2\frac{r_3-r_1}{r_3-r_2}\frac{q_d-r_2}{q_d-r_1}\right)x^2+1\right),$$

where r_1, r_2, r_3 are the roots of the polynomial x^3-3x+1 (or any other degree 3 polynomial $p(x)\in\mathbb{Q}[x]$ whose Galois group has order 3) and the parameters q_i are distinct rational numbers $q_4,\ldots,q_{2g+2}$ chosen so that $Aut(C)\cong\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$. Then

Theorem 1. I) *C is hyperelliptically defined over $\mathbb{Q}(r_1)$.*
II) *The field of moduli of C is $\mathbb{Q}$.*
III) *Let k be a subfield of the reals and C_k a curve of the form C_k: $y^2=q(x)$, where $q(x)$ is a polynomial with coefficients in k without multiple roots. Suppose that there is a birational isomorphism $f: C\rightarrow C_k$ defined over the compositum of the fields $\mathbb{Q}(r_1)$ and k, namely $k(r_1)$. Then k must contain the field $\mathbb{Q}(r_1)$.*

The online version of the original article can be found under doi:10.1007/s00013-005-1433-8.

Birkhäuser

This is a correction to Theorem 14 in the original article in which the statement III) was claimed to hold without imposing any restriction to the field of definition of f. In the proof we took a point $(a, b) \in C$ such that $f(a, b) = (x, y)$ with $x \in \mathbb{Q}$ (or, for that matter, in $k(r_1)$) and claimed that the field $k(r_1, i, a)$ is a Galois extension of k. This is not at all clear. However, if f is assumed to be defined over $k(r_1)$, then the point $(a, b) = (0, 1)$ clearly satisfies the condition since in that case $k(r_1, i, a) = k(r_1, i)$ and only the first of the cases discussed in Proposition 13 needs to be considered.

The statement III) as it was originally stated appears to be wrong. In fact, in [1] for $q_4 = 1, q_5 = 2, q_6 = 3$ an isomorphism (defined over a field extension of $\mathbb{Q}$ of higher degree) was found between C and a curve C_k with $k = \mathbb{Q}$. On the other hand, following a suggestion made by the referee, we observe that that statement would not be consistent with Proposition 4.2.2 in Huggins thesis [2].

Acknowledgements

We are grateful to Christophe Ritzenthaler who kindly pointed out the error to us and to our colleague Enrique González who carried out some computations in MAGMA for us.

References

[1] R. Lercier, C. Ritzenthaler, and J. Sijsling, *Fast computation of isomorphisms of hyperelliptic curves and explicit descent*. ANTS X: Proceedings of the tenth algorithmic number theory symposium, the Open Book Series 1, Mathematical Sciences Publishers, Berkely 2013.

[2] B. Huggins, Fields of moduli and fields of definition of curves. PhD thesis. University of California, Berkley (2005), http://arxiv.org/pdf/math/0610247.pdf.

Yolanda Fuertes and Gabino González-Diez
Departamento de Matemáticas,
U. Autónoma de Madrid,
E-28049 Madrid, Spain
e-mail: yolanda.fuertes@uam.es

Gabino González-Diez
e-mail: gabino.gonzalez@uam.es

Received: 2 July 2013