A CONTRIBUTION ON RATIONAL CUBIC GALOIS EXTENSIONS (REVISITED)

A. Paques
and
A. Solecki

RELATÓRIO TÉCNICO Nº 25/88

Abstract: In this paper we revisit cubic Galois extensions in order to expose their simple trigonometric origins in the rational case.

Universidade Estadual de Campinas
Instituto de Matemática, Estatística e Ciência da Computação
IMECC – UNICAMP
Caixa Postal 6065
13.081 – Campinas – SP
BRASIL

Dezembro – 1988

A CONTRIBUTION ON RATIONAL CUBIC GALOIS EXTENSIONS

A. Paques[∇] and A. Solecki[Δ]

∇ IMECC - UNICAMP, Caixa Postal 6065
13.081 - Campinas - SP, Brazil

Δ Departamento de Matemática, UFSC
88.049 - Florionópolis - SC, Brazil

We revisit cubic Galois extensions in order to expose their simple trigonometric origins in the rational case. Although the non trivial Galois extensions of prime degree of fields are fields ([6], Lemme 1.2), some results used in our proofs (like the one just cited) are formulated for rings. The general notion of Galois extension of a commutative ring considered here is due to Chase, Harrison and Rosenberg [1].

Let R be a commutative ring with unity and G be a finite group. An overring T of R is called a *Galois extension of* R *with the Galois group* Gal(T/R) $=G$ if G is a subgroup of Aut(T) and

i) the stabilizer $T^G = \{x \in T : \sigma(x) = x, \sigma \in G\}$ is equal to R,

ii) for any maximal ideal $p \subset T$ and any $\sigma \in G$, $\sigma \neq 1$ there exists $x \in T$ such that $\sigma(x) - x \notin p$.

The only extensions that we deal with here are cubic ones, that is when $G = Z_3$. We show that if L is a cubic Galois extension of $\mathbb{Q}$

then $L = \mathbb{Q}[c]$ with c any of three distinct cosines of angles γ_j, $j = 0,1,2$, such that the three vertices $e^{i\gamma_j} \in S^1$ yield an equilateral triangle (Proposition 1). A triangle with vertices $\omega^j e^{i\gamma}$ ($\omega^2 + \omega + 1 = 0$, $j=0,1,2$) corresponds in such way to a cubic Galois extension of $\mathbb{Q}$ if $\gamma \neq 0,\pi$ and for $\Gamma = 3\gamma$ the cosines of the three angles $\Gamma + j\frac{2\pi}{3}$ are in $\mathbb{Q}$ (Proposition 3 and Corollary). All angles Γ satisfying this condition are explicitly presented in terms of nonzero elements of the ring $\mathbb{Z}[\omega]$ (Proposition 2). When possible, the results are presented in a more general fashion, that is for a totally real algebraic extension K of $\mathbb{Q}$.

PROPOSITION 1. Let K be a field with char(K) either 0 or $p > 7$ and let L be a Galois extension of K with group $Gal(L/K) = \mathbb{Z}_3$. Then L is of the form $L = K(f) = K[X]/_{(f)}$ with $f(X) = X^3 - 3X - G$ for certain $G \in K$. If K is a totally real algebraic extension of $\mathbb{Q}$ then there exists $\Gamma \in \mathbb{R}/_{2\pi\mathbb{Z}}$ such that $G = 2\cos\Gamma$ and $2\cos(\frac{\Gamma}{3} + j\frac{2\pi}{3})$, $j = 0,1,2$, are roots of f.

PROOF. If L is trivial then it is isomorphic as a K-algebra to K^3 and all we need are three different elements $y_0, y_1, y_2 \in K$ such that $(X - y_0)(X - y_1)(X - y_2) = X^3 - 3X - G$; in virtue of our assumptions on the characteristic of K we may use the triple $\{-11/_7, -2/_7, 13/_7\}$ that gives $G = 286/_{343}$.

In the case when L is a field we use the fact that L has a normal normalized basis ([3], Satz 1), that is there exists a basis $\{x_0, x_1, x_2\}$ of L over K such that if σ denotes the generator of

$\mathbb{Z}_3$ we have $x_1 = \sigma(x_0)$, $x_2 = \sigma(x_1)$ and $x_0 + x_1 + x_2 = 1$, $x_0x_1 + x_1x_2 + x_2x_0 = 0$. Thus for $a = x_0x_1x_2 \in K$ we have $g(Z) = (Z - x_0)(Z - x_1)(Z - x_2) = Z^3 - Z - a$ and $L = K(g)$. Putting $Z = \frac{X+1}{3}$ we obtain $27g(Z) = X^3 - 3X - G$ with $G = 2 + 27a$.

Now, let K be a totally real algebraic extension of $\mathbb{Q}$. As the discriminant $2^2.3^3 - 3^3G^2$ is in $(K^*)^2$ (the standard symbol R^* standing for $R \setminus \{0\}$ for any ring R) we have $|G| < 2$ and define $\Gamma \in \mathbb{R}/_{2\pi\mathbb{Z}}$ by $\Gamma = \arccos \frac{G}{2}$. Note that multiplying by 2 the trigonometric identity $\cos 3\gamma = 4\cos^3\gamma - 3\cos\gamma$ and putting $3\gamma = \Gamma$, $2\cos\gamma = X$ we make it coincide with the equation $f(X) = 0$; therefore, $2\cos(\frac{\Gamma}{3} + j\,\frac{2\pi}{3})$, $j = 0,1,2$, are roots of f. ∎

A comment on the excluded finite characteristics: in the case of $p = 3$ the resulting polynomial $X^3 - G$ is not separable. For the remaining cases $p = 2,5$ or 7 the desired description of the trivial extension is possible if, and only if, $3 \pmod p$ is represented in K by the form $A^2 + AB + B^2$ with $(A-B)(2A+B)(A+2B) \neq 0$. This condition is satisfied for some extensions of $\mathbb{F}_p$ but — for example — not for $\mathbb{F}_p$ themselves.

Let R be a commutative ring with unity, G be an abelian finite group and $R[G]$ the group ring of G with coeficients in R. The elements of the Harrison group $T(R,G)$ ([2]) are $R[G]$-isomorphism classes of Galois extensions of R with the Galois group G. In the following description of $T(K, \mathbb{Z}_3)$ the field K is a totally real algebraic extension of $\mathbb{Q}$, O_K is its ring of integers, $\omega = -\frac{1}{2} + i\,\frac{\sqrt{3}}{2}$, $L = O_K[\omega]^*/_{O_K^*}$, $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ and $N = N_{K(\omega)/K}$

is the norm map: $N(s + t\omega) = s^2 - st + t^2$.

PROPOSITION 2. Let $S_K = K(\omega) \cap S^1$. There are group isomorphisms $T(K,\mathbb{Z}_3) \cong S_K / S_K^3$ and $L / L^3 \cong S_K / S_K^3$.

PROOF. Let σ generate $\mathbb{Z}_3$. For any commutative ring R with unity and any $j \in \mathbb{Z}$ the formula $\nu_j(\sigma) = \sigma^j$ induces an endomorphism ν_j of the R-algebra $R[\mathbb{Z}_3]$. Let $W_R = \{x \in R[\mathbb{Z}_3]: x.\nu_{-1}(x) = 1$ and $\nu_0(x) = 1\}$. It is a subgroup of the group $U(R[\mathbb{Z}_3])$ of the units of $R[\mathbb{Z}_3]$. It follows from Satz 4.1 of [4] that when R is a local ring with $3 \in U(R)$ then there exists a group isomorphism $W_R / W_R^3 \cong T(R, \mathbb{Z}_3)$.

Now, let $R = K$ be a totally real algebraic extension of $\mathbb{Q}$ and define a ring homomorphism $\chi_j : K[\mathbb{Z}_3] \longrightarrow K(\omega)$ by extending the formula $\chi_j(\sigma) = \omega^j$ for $j \in \mathbb{Z}$ to the ring $K[\mathbb{Z}_3]$. The proposition will be proved when we show that $W_K \cong S_K$ and $L \cong S_K$.

If $w = k_0 + k_1\sigma + k_2\sigma^2 \in W_K$ we have $k_0 + k_1 + k_2 = 1$ and $k_0k_1 + k_1k_2 + k_2k_0 = 0$; consequently, the image $\chi_1(w) = (k_0 - k_2) + (k_1 - k_2)\omega$ in $K(\omega)$ satisfies $N(\chi_1(w)) = 1$. So, restricting χ_1 to W_K we get a group homomorphism $\chi_1 : W_K \longrightarrow S_K$. Clearly, it is injective. On the other hand, if $a + b\omega \in S_K$ then easy verification shows that we have $w \in W_K$ and $\chi_1(w) = a + b\omega$ for $w = [(1 + 2a - b) + (1 - a + 2b) + (1 - a - b)\sigma^2]$ so that χ_1 is surjective.

To complete the proof we define the mapping

$\varphi : L \longrightarrow S_K$, $[\ell] \longmapsto \frac{\ell^2}{N(\ell)}$, where $[\ell]$ is the class of $\ell \in O_K[\omega]^*$ modulo O_K^*. For $k \in O_K^*$ we have $k^2 = N(k)$ and therefore φ is a well-defined homomorphism. Since $N(\ell) = \ell^2$ if, and only if, $\ell \in O_K^*$ we have the injectivity of φ. To prove the surjectivity of φ, note first that $-1 \in S_K$ is the image of the class of $1 + 2\omega \in O_K[\omega]^*$. Then let $s = \cos\alpha + i\sin\alpha \in S_K$ with $\alpha \neq 0, \pi$. It is enough to exhibit any $k \in K(\omega)$ with $\arg(k) = \frac{\alpha}{2}$ because K is the field of fractions of O_K and for certain $z \in O_K$ we will have $zk \in O_K[\omega]^*$. Well, take $k = 1 + s$. Obviously, $k \in K(\omega)$ and by recalling the identity $\operatorname{tg}\frac{\alpha}{2} = \frac{\sin\alpha}{1+\cos\alpha}$ (or by drawing a rhomb with vertices $0, 1, s, 1+s$) we see that $\arg(k) = \frac{\alpha}{2}$. ∎

PROPOSITION 3. $S_K = \{e^{i\Gamma} \in S^1 : \cos(\Gamma + j\frac{2}{3}) \in K \text{ for } j = 0,1,2\}$.

PROOF. If $s = \cos\Gamma + i\sin\Gamma \in S^1$ and also $s = a + b\omega \in K(\omega)$ then we have $a - \frac{b}{2} = \cos\Gamma \in K$; but as $\frac{3}{2}b = \sqrt{3}\sin\Gamma \in K$ we also have $\cos(\Gamma \pm \frac{2\pi}{3}) \in K$. Conversely, $\cos(\Gamma + j\frac{2\pi}{3}) \in K$ for $j = 0,1,2$ implies $\sqrt{3}\sin\Gamma \in K$, hence $\omega\sqrt{3}\sin\Gamma \in K(\omega)$ and, finally, $i\sin\Gamma \in K(\omega)$. Therefore $\cos\Gamma + i\sin\Gamma \in K(\omega)$. ∎

COROLLARY. Let $e^{i\Gamma} \in S_K \setminus \{\pm 1\}$. We have $K(\cos\frac{\Gamma}{3}) = K(f)$ with $f(X) = X^3 - 3X - G$, where $G = \frac{2s^2 + 2st - t^2}{s^2 - st - t^2}$ with $\varphi([s + t\omega]) = e^{i\Gamma}$.

Moreover, $K(\cos\frac{\Gamma}{3})$ is a Galois extension of R.

PROOF. For $e^{i\Gamma} \in S_K \setminus \{\pm 1\}$ select $\ell = s + t\omega$ with $\arg(\ell) = \frac{\Gamma}{2}$; thus

$tg \frac{\Gamma}{2} = \frac{\sqrt{3}\, t}{2s - t}$. Use the identity that expresses $\cos\Gamma$ by $tg^2 \frac{\Gamma}{2}$ and then the trigonometric identity used in the proof of Proposition 1. As $G = 2\cos\Gamma$, the first claim is proved. The second one is settled by noting that for $\Gamma \neq 0, \pi$ the discriminant $(6\sqrt{3} \sin\Gamma)^2$ of f is a non zero square in K. ∎

We would like to mention that the presentation of elements of $T(K, \mathbb{Z}_3)$ in terms of elements $\ell = s + t\omega \in O_K[\omega]^*$, given in Proposition 2, coincides with the description given in [5] where K is any field with $char(K) \neq 3$ and extensions fields are parametrized by $k \in K$ which appears in the polynomial $f_k(X) = X^3 - 3kX^2 + 3(k-1)X + 1$. If K is a totally real algebraic extension of $\mathbb{Q}$ then the passage from one description to another is $\ell = s + t\omega \longmapsto k = \frac{s}{t}$.

ACKNOWLEDGEMENT. We wish to express our gratitude to the referee who improved some results and brought us to simplify our proofs.

REFERENCES

[1] S.U. CHASE, D.K. HARRISON, A. ROSENBERG, Galois Theory and Galois Cohomology of commutative rings, Memoirs of AMS 52 (1965), 15-33.

[2] D.K. HARRISON, Abelian extensions of commutative rings, Memoirs of AMS 52 (1965), 1-14.

[3] I. KERSTEN, J. MICHALIČEK, Kubische Galoiserweiterungen mit Normalbasis, Comm. in Algebra 9 (1981), 1863-1871.

[4] I. KERSTEN, J. MICHALIČEK, Galoiserweiterungen der Ordnung p mit Normalbasis, Comm. in Algebra 10 (1982), 695-718.

[5] I. KERSTEN, J. MICHALIČEK, A characterization of Galois field extensions of degree 3, Comm. in Algebra 15, (1987), 927-933.

[6] A. MICALI, A. PAQUES, Sur le groupe des extensions cycliques, J. of Algebra 63 (1980), 268-278.

RELATÓRIOS TÉCNICOS — 1988

01/88 - **A Linear Continuous Transportation Problem** - *Enrique D. Andjel, Tarcísio L. Lopes* and *José Mario Martínez.*

02/88 - **A Splitting Theorem for Complete Manifolds With Non Negative Curvature Operator** - *Maria Helena Noronha.*

03/88 - **Mathematical Physics of the Generalized Monopole without String** - *W. A. Rodrigues Jr., M. A. Faria-Rosa, A. Maia Jr.* and *E. Recami.*

04/88 - **A Family of Quasi-Newton Methods with Direct Secant Updates of Matrix Factorizations** - *José Mário Martínez.*

05/88 - **Rotation Numbers of Differential Equations. A Framework in the Linear Case** - *Luis San Martin.*

06/88 - **A Geometrical Theory of non Topological Magnetic Monopoles** - *Marcio A. Faria-Rosa* and *Waldyr A. Rodrigues Jr.*

07/88 - **Cosmic Walls and Axially Symmetric Sigma Models** - *Patricio S. Letelier* and *Enric Verdaguer.*

08/88 - **Verificação do Nível de Enlace do Protocolo X-25** - *Célio C. Guimarães* e *Edmundo R. M. Madeira.*

09/88 - **A Numerically Stable Reduced-Gradient Type Algorithm for Solving Large-Scale Linearly Constrained Minimization Problems** - *Herminio Simões Gomes* and *José Mário Martínez.*

10/88 - **On Integral Bases of Some Ring of Integers** - *Nelo D. Allan.*

11/88 - **Generating Inexact-Newton Methods Using Least Change Secant Update Procedures** - *José Mario Martínez.*

12/88 - **Polarized Partition Relations of Higher Dimension** - *Walter Alexandre Carnielli* and *Carlos Augusto Di Prisco.*

13/88 - **Teoria e Prática no Planejamento de Experimentos** - *Armando M. Infante.*

14/88 - **On Closed Twisted Curves** - *Sueli I. R. Costa.*

15/88 - **Green's Function and Isotropic Harmonic Oscillator** - *E. Capelas de Oliveira.*

16/88 - **A Hopf Bifurcation Theorem for Evolution Equations of Hyperbolic Type** - *Aloisio Freiria Neves* and *Hermano de Souza Ribeiro.*

17/88 - **Nonnegatively Curved Submanifolds in Codimension Two** - *Maria Helena Noronha.*

18/88 - **A Comment on the Twin Paradox and the Hafele-Keating Experiment** - *W. A. Rodrigues Jr.* and *E. C. Oliveira.*

19/88 - **Limiting Properties of the Empirical Probability Generating Function of Stationary Random Sequences and Processes** - *Mauro S. Marques* and *Victor Pérez-Abreu.*

20/88 - **Linearization of Bounded Holomorphic Mappings on Banach Spaces** - *Jorge Mujica.*

21/88 - **Quasi-Newton Methods for Solving Underdetermined Nonlinear Simultaneous Equations** - *José Mario Martínez.*

22/88 - **Fifth Force, Sixth Force, and all that: a Theoretical (Classical) Comment** - *Erasmo Recami* and *Vilson Tonin-Zanchin.*

23/88 - **On Primitive Element and Normal Basis for Galois *p*-Extensions of a Commutative Ring** - *A. Paques.*

24/88 - **Sur L'Existence D'Élément Primitif et Base Normale** - *Antonio Micali* and *A. Paques.*