Characterizing cyclic quartic extensions by automorphism polynomials

Michelle Manes* and Katherine Stange

University of Hawai‘i at Mānoa
mmanes@math.hawaii.edu
http://math.hawaii.edu/~mmanes
Preliminary report*

8 January, 2016

Characterizing cyclic quartic extensions by automorphism polynomials

Michelle Manes* and Katherine Stange

University of Hawaiʻi at Mānoa
mmanes@math.hawaii.edu
http://math.hawaii.edu/~mmanes

Preliminary report*
*Now with extra preliminary

8 January, 2016

Kummer Theory

If $\mu_n \subset K$, then there is a simple description of the exponent n abelian extensions of K.

$$\text{abelian extensions of } K \text{ of exponent } n$$
$$\updownarrow$$
$$\text{subgroups of } K^*/(K^*)^n$$

Morton: Cyclic cubic fields

For any field K of characteristic $\neq 2$, we have

$$\text{abelian extensions of } K \text{ of exponent } 3$$
$$\updownarrow$$
$$\text{certain groups of linear fractional transformations}$$

Setup

Let F/K be a cycle cubic extension and $\mathrm{Gal}(F/K) = \langle\sigma\rangle$. Idea:

- $F = K(\theta)$ for some primitive element.
- There is some polynomial $f(x) \in K[x]$ of degree < 3 such that $\sigma(\theta) = f(\theta)$.
- If $\zeta_3 \notin K$, then can take $f(x) = x^2 + c$ with θ a point of primitive period 3 for f.
- $[F : K] = 3$ and cyclic means that θ is a root of an irreducible cubic factor of $\Phi_3^*(x, c)$.
- Then $f(x) = x^2 - \frac{1}{4}(s^2 + 7)$. and

$$\Phi_3^* = g(x, s)g(x, -s), \quad \text{where}$$

$$g(x, s) = x^3 + \frac{1}{2}(1-s)x^2 - \frac{1}{4}(s^2+2s+9)x + \frac{1}{8}(s^3+s^2+7s-1).$$

Cyclic cubic fields

Theorem (Morton, 1992)

Let F/K be an abelian extension of exponent 3 and rank r, and suppose char $K \neq 2$. *Then*

$$F = K(\theta_1, \theta_2, \ldots, \theta_r)$$

where θ_i is any root of the irreducible polynomial $g(x, s_i)$ for suitable values $s_i \in K$.
Conversely, if the $s_i \in K$ are independent, then the polynomials $g(x, s_i)$ are all irreducible over K and the extension

$$F = K(\theta_1, \theta_2, \ldots, \theta_r)/K$$

has degree 3^r and exponent 3.

Morton’s comment

“It would be interesting to generalize the results given here to cyclic extensions of any degree. . . ”

Setup

Let F/K be a cyclic quartic extension. Assume $i \notin K$ and char $K \neq 2, 3$. Let $\mathrm{Gal}(F/K) = \langle \sigma \rangle$.

There is a unique quadratic subfield F_2 such that

- $F_2 = F^{\langle \sigma^2 \rangle}$.
- $F = K(\theta)$ with $\theta^2 \in F_2$.

Proposition

With this notation, $\sigma(\theta) = f(\theta)$ where $f \in K[x]$ has the form $f(x) = ax^3 + bx$.

Proof.

Let $p(x)$ be the minimal polynomial of θ. Note $\deg(p) = 4$.

$$\begin{aligned} f^2(x) &\equiv -x \pmod{p} \\ f^3(x) &= f^2(f(x)) \equiv -f(x) \pmod{p} \\ &= f(f^2(x)) \equiv f(-x) \pmod{p} \end{aligned}$$

$$-f(x) \equiv f(-x) \pmod{p}$$

Since $\deg(f) < \deg(p)$, this is equality. So $f(x) = ax^3 + bx$. $\square$

Note: $i \notin K \implies a \neq 0$.

Upshot

We have $f = ax^3 + bx$ and θ a point of primitive period 4 for f. So θ is a root of an irreducible quartic factor of Φ_4^*.

But even more is true:

- f has a nontrivial automorphism $h(x) = -x$.
- Since $f^2(\theta) = -\theta$, in fact θ is a root of an irreducible quartic factor of the "*h*-tuned dynatomic polynomial"

$$\begin{aligned}\Psi_4^* &= \frac{f^2(x) + x}{x} \\ &= a^4x^8 + 3a^3bx^6 + 3a^2b^2x^4 + (ab^3 + ab)x^2 + (b^2 + 1).\end{aligned}$$

Proposition

The h-tuned dynatomic polynomial Ψ_4^* factors as a product of two quartics if and only if $b = \frac{-3m^2+2m-3}{m^2-1}$ for some $m \in K \setminus \{\pm 1\}$. The two quartics are irreducible provided that m is not of the form

$$\frac{t^2+1}{t^2-1} \quad \text{or} \quad \frac{s^2+8s+11}{5-s^2}$$

for any $s, t \in K$.

Proof sketch

Let θ be a root of Ψ_4^*. Define the norm of a cycle:

$$n = \prod_{j=0}^{3} f^j(\theta).$$

A necessary condition for Ψ to split into two quartic factors is that the two four-cycles have K-rational norm.

Define a quadratic polynomial

$$\eta(x) = (x - n_1)(x - n_2) = x^2 + Ax + B$$

whose roots are these two norms.

Use the fact that $\eta(x) \equiv 0 \pmod{\Psi_4^*}$ to find A and B in terms of a and b.

Proof sketch

$\eta(x)$ has rational roots when the discriminant is a square in K, which happens when $b^2 - 8$ is a square.

Parameterize the curve $d^2 = b^2 - 8$ to get that b must be of the form $\frac{-3m^2+2m-3}{m^2-1}$.

In this case, the two quartic factors of Ψ_4^* are both even. Use the same idea to show that they factor further iff m is of the form

$$\frac{t^2+1}{t^2-1} \quad \text{or} \quad \frac{s^2+8s+11}{5-s^2}.$$

Comparison

Morton:
For $f(x) = x^2 - \frac{1}{4}(s^2 + 7)$, we have

$$\Phi_3^* = g(x,s)g(x,-s), \quad \text{where}$$

$$g(x,s) = x^3 + \tfrac{1}{2}(1-s)x^2 - \tfrac{1}{4}(s^2+2s+9)x + \tfrac{1}{8}(s^3+s^2+7s-1).$$

For suitable choices of $s \in K$, roots of g generate cyclic cubic extensions.

Moreover, every cyclic cubic extension of K arises in this way when $\zeta_3 \notin K$.

Comparison

M-Stange:

For $f(x) = ax^3 + \frac{-3m^2+2m-3}{m^2-1}x$, we have

$$\Psi_4^* = g(x,a,m)g\left(x, a, \frac{3\mathrm{m}-1}{\mathrm{m}-3}\right), \quad \text{where}$$

$$g(x,a,m) = x^4 - \frac{4a\left(m^2+1\right)}{(m-1)(m+1)}x^2 + \frac{2\left(m^2+1\right)}{(m-1)^2}.$$

For suitable choices of $m \in K$, roots of g generate cyclic quartic extensions.

Moreover, every cyclic quartic extension of K arises in this way when $i \notin K$.

Independence condition

To get something like the one-to-one correspondence, we need to know when two parameters give the same extension.

- Kummer theory: $K\left(\sqrt[n]{\alpha}\right) = K\left(\sqrt[n]{\beta}\right)$ iff $\alpha/\beta \in (K^*)^n$
- Morton: The roots of $g(x, s)$ and $g(x, v)$ — that is, the period-3 points of $x^2 - \frac{1}{4}(s^2 + 7)$ and $x^2 - \frac{1}{4}(v^2 + 7)$ — generate the same cyclic cubic extension iff s and v are in the same K-orbit of a certain group of linear fractional transformations.
- M.-Stange: The roots of $g(x, 1, m)$ and $g(x, 1, n)$ — that is, the period-4 points of $x^3 + \frac{-3m^2+2m-3}{m^2-1}x$ and $x^3 + \frac{-3n^2+2n-3}{n^2-1}x$ — generate the same cyclic quartic extension iff m and n are in the same K-orbit of a certain group of linear fractional transformations.
  Pay no attention to the twist parameter a...

Maps generating the same extension

We know: If $\phi \sim_{/K} \psi$ then the period n points of ψ and ϕ generate the same extension of K for every n.

What can we say if the period-n points for ϕ and ψ generate the same extension for some fixed n? (Probably nothing.)

But what if we narrow it down even further?

- cyclic extension?
- ϕ and ψ in one-parameter family?

- The fixed points of $x^2 + b$ and $x^2 + c$ generate the same extension iff b and c are in the same K-orbit of a certain group of linear fractional transformations.

- The period-2 points of $x^2 + b$ and $x^2 + c$ generate the same extension iff b and c are in the same K-orbit of a certain group of linear fractional transformations.

- Morton's result for cyclic cubic extensions generated by period-3 points of $x^2 - \frac{1}{4}(s^2 + 7)$.

Over $\mathbb{Q}$: If the period-4 points of $x^2 + c$ generate a cyclic quartic extension, then $c = -(t^3 + 3t + 4)/4t$. Different choices for the parameter t yield non-isomorphic fields.

Morton: The period-4 points of $x^2 + c$ generate a cyclic quartic extension iff c has this form and the polynomial

$$x^4 - t^2x^3 - (t^3 + 2t^2 + 4t + 2)x^2 - t^2x + 1$$

is irreducible.

Washington: The discriminant of the cyclic quartic field is $t^2(t+2)^2(t^2+4)^3$.

For $n \geq 5\ldots$

- Only finitely many choices of c such that period n points of $x^2 + c$ generate a cyclic extension.
- For n sufficiently large, probably (?) only $c = 0, -2$.
- Probably (?) all such c generate distinct fields.

- The fixed points of $x^3 + ax$ and $x^3 + bx$ generate the same extension iff a and b are in the same K-orbit of a certain group of linear fractional transformations.
- The period-2 points of $x^3 + ax$ and $x^3 + bx$ generate the same extension iff b and c are in the same K-orbit of a certain group of linear fractional transformations.
- M-Stange result for cyclic quartic extensions generated by period-4 points of $x^3 + \frac{-3m^2+2m-3}{m^2-1}x$.