Applying a Galois Transformation to the Roots of a Polynomial

Ken McMurdy
Ramapo College of New Jersey
November 10, 2013

1 Introduction

Suppose that a polynomial $f(x)$ is defined over a field $K$, and that all of its roots lie in some fixed algebraic closure $\overline{K}$. For the sake of simplicity, assume further that $f$ is monic. In other words, suppose that

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \quad a_i \in K$$

$$= (x - r_1)(x - r_2)\cdots(x - r_n) \quad r_i \in \overline{K}.$$

It is not uncommon to seek the related polynomial, $f_T(x)$, whose roots are precisely $T(r_i)$, where $T : \overline{K} \to \overline{K}$ is some rational function.

$$f_T(x) = (x - T(r_1))(x - T(r_2))\cdots(x - T(r_n))$$

One obvious method for obtaining $f_T(x)$ would be to factor $f(x)$ and apply the definition. However, factoring $f(x)$ first can be extremely time-consuming, may require working over a larger field, and is in many cases unnecessary.

For example, suppose that we simply want to add a constant $c \in \overline{K}$ to each root, i.e., apply the transformation, $T(x) = x + c$. In this case it is easy to see that $f_T(x) = f(x - c)$. So we can compute $f_T(x)$ without factoring at all, but rather by substituting $(x - c)$ for $x$ and expanding. Similarly, if we want to multiply each root by a nonzero constant $c \in \overline{K}$, we simply take $f_T(x) = c^n f(x/c)$. Finally, if the roots are all nonzero and we want to reciprocate them, i.e., apply $T(x) = x^{-1}$ to all of the roots, well that is just given by $f_T(x) = a_0^{-1}x^n f(1/x)$. By combining these rules, it is possible to transform the roots via any (invertible) affine transformation over $\overline{K}$.

$$T(x) = \frac{ax + b}{cx + d}$$

More generally, suppose now that $T$ is any rational function defined over $\overline{K}$, and we want to compute $f_T(x)$ without factoring $f(x)$ first. The problem can still be done, by interpreting the coefficients of $f(x)$ as elementary symmetric
functions of the roots (see [DF, §14.6] or [La1, V, §9]). For example, consider the following polynomial with rational coefficients:\(^1\)

\[ f(x) = x^3 + \frac{8}{3}x^2 - 11x + \frac{10}{3} = (x - \frac{1}{3})(x - 2)(x + 5) \]

Suppose we want to square the roots of \(f(x)\), i.e., apply the transformation, \(T(x) = x^2\), to the roots, without using the factorization. Interpreting the coefficients as elementary symmetric functions of the roots (as in [DF, Eq. 14.13]), we have the following equations.

\[
-\frac{8}{3} = s_1 := r_1 + r_2 + r_3 \\
-11 = s_2 := r_1r_2 + r_1r_3 + r_2r_3 \\
-\frac{10}{3} = s_3 := r_1r_2r_3
\]

Now, set \(f_T(x) = x^3 + b_2x^2 + b_1x + b_0\). Thinking of these coefficients as elementary symmetric functions in the new roots, \(r_1^2\), \(r_2^2\) and \(r_3^2\), leads to the following equations.

\[
b_2 = -r_1^2-r_2^2-r_3^2 = -s_1^2+2s_2 = -\frac{262}{9} \\
b_1 = r_1^2r_2^2+r_1^2r_3^2+r_2^2r_3^2 = s_2^2-2s_1s_3 = \frac{929}{9} \\
b_0 = -r_1^2r_2^2r_3^2 = -s_3^2 = -\frac{100}{9}
\]

One sees immediately by factoring \(f_T(x)\) that this is correct.

\[
x^3 - \frac{262}{9}x^2 + \frac{929}{9}x - \frac{100}{9} = (x - \frac{1}{3})(x - 4)(x - 25)
\]

The above method does in fact work for any rational \(T(x)\). Indeed, any elementary symmetric function in the \(T(r_i)\) must still be a symmetric function in the original \(r_i\). Hence it must be a rational function in the original elementary symmetric functions, \(s_i\) (by [DF, §14, Cor 31] or [La1, Thm 9.1]). Thus the coefficients of \(f_T(x)\) can be computed in general from the coefficients of \(f(x)\), precisely as in the previous example. For an illustrative example, we recommend as an exercise applying the rational function, \(T(x) = (x^2 - 1)/(x^2 + 1)\), to the roots of the cubic polynomial \(f(x)\) given above. For the first step, we have

\[
T(r_1) + T(r_2) + T(r_3) = \frac{3r_1^2r_2^2r_3^2 + r_1^2r_2^2 + r_1^2r_3^2 + r_2^2r_3^2 - r_1^2 - r_2^2 - r_3^2 - 3}{r_1^2r_2^2 + r_1^2r_3^2 + r_2^2r_3^2 + r_1r_2r_3 + r_1^2 + r_2^2 + r_3^2 + 1}
\]

\[
= \frac{3s_3^2 + s_2^2 - 2s_1s_3 + s_1^2 + 2s_2 - 3}{s_3^2 + s_2^2 - 2s_1s_3 + s_1^2 - 2s_2 + 1} = \frac{940/9}{1300/9} = \frac{47}{65}.
\]

So \(b_2 = -\frac{47}{65}\) (which is correct).

Unfortunately, however, this method for computing \(f_T(x)\) is very computationally complex. We point out, in particular, that the complexity grows with

\(^1\)This polynomial was constructed by randomly choosing its roots. However, all nontrivial factoring and other additional calculations for the remainder of the paper have been done using the SAGE computational software package (see [Sa]).
the degree of \( f \), and not just with the degree of \( T \). Moreover, if the calculations were to be carried out exactly as above, one would need to do symbolic calculations over the polynomial ring with \( n \) indeterminates. The goal of this brief note is to present an alternative approach, which will work for many rational functions and is superior in both complexity and simplicity.

2 Galois Transformations

To motivate the preferred method for computing \( f_T(x) \), let us revisit the problem of squaring the roots of the polynomial from the previous section. Rather than compute \( f_T(x) \) directly in this case, it is actually much easier to compute \( f_T(x^2) \) first.

\[
f_T(x^2) = (x^2 - r_1^2)(x^2 - r_2^2)(x^2 - r_3^2)
= (x - r_1)(x - r_2)(x - r_3)(x + r_1)(x + r_2)(x + r_3)
= (-1)^3 f(x) f(-x)
= - (x^3 + \frac{8}{3}x^2 - 11x + \frac{10}{3}) (-x^3 + \frac{8}{3}x^2 + 11x + \frac{10}{3})
= x^6 - \frac{262}{9}x^4 + \frac{929}{9}x^2 - \frac{100}{9}
\]

\[
f_T(x) = x^3 - \frac{262}{9}x^2 + \frac{929}{9}x - \frac{100}{9}
\]

Obviously this method for squaring the roots of a polynomial will work for polynomials of arbitrary degree. The complexity goes up with the degree, but in a very predictable way. Moreover, we only needed to do symbolic calculations in a univariate polynomial ring. Can we do something similar for more general transformations?

The answer is “yes,” and the key is to think in terms of elementary Galois theory.\(^2\) Think of the function field, \( K(t) \), as a base field, and think of \( K(t)[x] \) as a degree two Galois extension generated by a root \( x \) of the irreducible polynomial \( X^2 - t \). With this perspective, \( x \) and \( -x \) are Galois conjugates in the larger field (see [DF, pg. 487]). Indeed, since \( t = x^2 \), the minimal polynomial for \( x \) over \( K(t) \) factors over the larger field as

\[
X^2 - t = X^2 - x^2 = (X - x)(X + x).
\]

So \( K(t)[x] \) is the splitting field for the irreducible polynomial \( X^2 - t \) over \( K(t) \) (see [DF, Ch 14, Thm 13], [La1, VII, §3]). Hence the middle line from the above calculation, \( f_T(x^2) = (-1)^3 f(x) f(-x) \), can be rephrased as \( f_T(t) = (-1)^3 N(x) \), where \( N \) is the usual norm (as in [La1, VIII, §5], [DF, §14.2, Ex. 17]). We only need to formalize this setup, to see that our approach does in fact generalize to a large category of transformations.

Definition 2.1. Let \( T(x) = p(x)/q(x) \) be a rational function with coefficients in some fixed field \( K \). We say that \( T \) is a Galois transformation if \( K(t)[x]/K(t) \)

\(^2\)We cite [DF, Ch 13, 14] and [La1, VII, VIII], as excellent references for this material.
defines a Galois extension of function fields when we set \( t = T(x) \). More precisely, the polynomial, \( h(X) := q(X)t - p(X) \), must be irreducible over \( K(t) \), \( K(t)[x] \) must be the splitting field of \( h(X) \), and \( h(X) \) must have distinct roots over the larger field. We say that \( T \) is potentially Galois if this condition holds after finite base extension, i.e., when we consider \( T \) to be defined over some finite extension \( L \supseteq K \).

**Example 2.2.** For an easy example of a transformation that is potentially Galois but not Galois, consider \( T(x) = x^3 \) over \( K = \mathbb{Q} \). Setting \( t = x^3 \), we may only factor \( X^3 - t \) over \( K(t)[x] \) as

\[
X^3 - t = X^3 - x^3 = (X - x)(X^2 + xX + x^2).
\]

The polynomial splits completely over \( L(t)[x] \), however, where \( L = \mathbb{Q}(\sqrt{-3}) \).

\[
X^3 - t = (X - x)(X - \zeta x)(X - \zeta^2 x) \\
\zeta = \frac{-1 + \sqrt{-3}}{2}
\]

**Example 2.3.** For an example of a transformation that is not even potentially Galois, consider

\[
T(x) = \frac{x^3 - 5x - 1}{x^2 + 2}
\]

over \( K = \mathbb{Q} \). Setting \( T(x) = 1 \) leads to the following polynomial equation.

\[
x^3 - x^2 - 5x - 3 = (x - 3)(x + 1)^2 = 0
\]

Thus, in the language of algebraic curves, the \( t = 1 \) point on \( \mathbb{P}^1(L) \) will split in the extension (regardless of \( L \)), into two points with \( x = 3 \) and \( x = -1 \) respectively. Since these two points in the same fiber do not have the same ramification index, the extension can not possibly be Galois. Alternatively, in the language of commutative algebra, \( (t - 1) \) is a prime ideal in the Dedekind domain, \( L[t] \). Hence, if the extension were Galois, the two prime ideals lying over it, \( (x - 3) \) and \( (x + 1) \), would have to have the same ramification index. (See [La2, I, §7, Cor. 2], for example.)

**Lemma 2.4.** Let \( T(x) = p(x)/q(x) \) be a Galois transformation over a field \( L \). Define \( h(X) \) as above, and let \( c(t) \) denote the leading coefficient of \( h(X) \). Let \( \{\alpha_1, \ldots, \alpha_m\} \) denote the distinct Galois automorphisms of \( L(t)[x]/L(t) \), where \( x \) is a root of \( h(X) \). Then for any \( r \in L \) we have

\[
t - T(r) = \frac{(-1)^m c(t)}{q(r)} \cdot [(\alpha_1(x) - r)(\alpha_2(x) - r) \cdots (\alpha_m(x) - r)].
\]

**Proof.** Since \( r \in L \), and \( L \) is fixed by each \( \alpha_i \), we have

\[
(\alpha_1(x) - r)(\alpha_2(x) - r) \cdots (\alpha_m(x) - r) = \alpha_1(x - r)\alpha_2(x - r) \cdots \alpha_m(x - r),
\]

which is the norm of \( x - r \). But since \( x - r \) generates the full degree \( m \) Galois extension, its norm must also equal \((-1)^m \) times the constant term of its minimal polynomial. In this case, that is the constant term of

\[
f_{\text{min}}(x - r) = \frac{1}{c(t)} h(X + r) = \frac{1}{c(t)} [q(X + r)t - p(X + r)].
\]
Using the fact that $p$ and $q$ are polynomials, this term is given by
\[
\frac{1}{c(t)}[q(r)t - p(r)] = \frac{q(r)}{c(t)} \left[ t - \frac{p(r)}{q(r)} \right] = \frac{q(r)}{c(t)}(t - T(r)).
\]

**Theorem 2.5.** Let $f(x)$ be a monic polynomial over a field $K$. Suppose that $T(x) = p(x)/q(x)$ is a potentially Galois transformation over $K$. Choose any finite extension $L \supseteq K$, containing the roots of $f$, and over which $T$ becomes Galois. Let $c(t)$ be the leading coefficient of $h(X) := q(X)t - p(X)$. Then
\[
f_T(t) = \epsilon \cdot [c(t)]^n \cdot f(\alpha_1(x))f(\alpha_2(x)) \cdots f(\alpha_m(x)),
\]
where the $\alpha_i$ are as above and $\epsilon = (-1)^m \prod_i q(r_i)^{-1}$ (which is in $L$).

**Proof.** This follows from factoring the right hand side, rearranging the factors, and applying the lemma.

\[
f(\alpha_1(x))f(\alpha_2(x)) \cdots f(\alpha_m(x)) = \prod_{j=1}^m f(\alpha_j(x))
= \prod_{j=1}^m \prod_{i=1}^n (\alpha_j(x) - r_i)
= \prod_{i=1}^n \prod_{j=1}^m (\alpha_j(x) - r_i)
= \prod_{i=1}^n \frac{q(r_i)}{\epsilon^{-1} c(t)^{-n} f_T(t)}(t - T(r_i))
= \epsilon^{-1} [c(t)]^{-n} f_T(t)
\]

In practice, the $L$ need not be made explicit, and the $\epsilon$ can be ignored altogether. In order to apply the theorem, all we really need is the explicit formula for each $\alpha_i(x)$. Indeed, once we are able to write
\[
[c(t)]^n \cdot f(\alpha_1(x))f(\alpha_2(x)) \cdots f(\alpha_m(x))
\]
as a polynomial in $t$, it is trivial to divide through by the leading coefficient to obtain the monic polynomial $f_T(t)$. This first step, however, of rewriting the ostensible function of $x$ as a polynomial in $t$, bears some mentioning. To be more precise, if we substitute $t = T(x)$ into (1), what we really have is a constant multiple of $f_T(T(x))$. Unfortunately, knowing that this can be rewritten as a polynomial in $t$ alone (via the substitution $t = T(x)$) does not tell us how to efficiently do it. One approach to solving this “inverse substitution problem” is with a recursive algorithm that we now describe.
First suppose that \( p(x) \) has a root \( \xi \) in some extension of \( K \). In this case, the coefficients of \( f_T(t) \) can be computed in ascending order, by starting with \( f_T(T(x)) \) and then recursively (1) evaluating at \( x = \xi \), (2) subtracting off the result, and (3) dividing by \( T(x) \). The reason this works is that \( T(\xi) = 0 \). So the process is equivalent to recovering the coefficients of

\[
f_T(t) = b_n t^n + b_{n-1} t^{n-1} + \cdots + b_2 t^2 + b_1 t + b_0
\]

by recursively (1) evaluating at \( t = 0 \), (2) subtracting off the result, and (3) dividing by \( t \) (which clearly yields the coefficients, \( b_0, b_1, b_2, \text{etc.} \)). The only case in which our approach will fail is when \( p(x) \) is a constant. Unless \( T \) is constant, however, this implies that \( q(x) \) must have a root in some \( L \). So in this case we may apply the transformation \( 1/T \) to the roots first (using the above method), and then reciprocate them.

Before we present our primary example, let us revisit the two earlier examples involving the cubic polynomial,

\[
f(x) = x^3 + \frac{8}{3} x^2 - 11 x + \frac{10}{3} = (x - \frac{1}{3}) (x - 2) (x + 5).
\]

First take \( T(x) = x^2 \), so that \( p(x) = x^2 \), \( q(x) = 1 \), and \( h(X) = -X^2 + t \). This is a Galois transformation over \( \mathbb{Q} \) in the sense of Definition 2.1, and the conjugates of \( x \) are \( x \) and \( -x \). Therefore, applying the theorem, we have

\[
f_T(t) = \epsilon \cdot [c(t)]^n \cdot f(x) f(-x)
= \epsilon \cdot (-1)^3 f(x) f(-x)
= -\epsilon \left( -x^6 + \frac{262}{9} x^4 - \frac{929}{9} x^2 + \frac{100}{9} \right)
= t^3 - \frac{262}{9} t^2 + \frac{929}{9} t - \frac{100}{9}.
\]

Note that \( \epsilon \) is indeed 1 from the definition, but it wasn’t actually necessary to compute \( \epsilon \). Also, the conversion from \( x \)’s to \( t \)’s at the end was easy because we were in the special case of \( t = x^2 \). However, it certainly could be done using the recursive method described above with \( \xi = 0 \).

The second example, involving the same \( f(x) \) but with the transformation, \( T(x) = (x^2 - 1)/(x^2 + 1) \), is more enlightening. Now,

\[
h(X) = (X^2 + 1) t - X^2 + 1 = (t - 1) X^2 + t + 1,
\]

and so \( c(t) = t - 1 \). Again, the extension is of degree 2 and hence Galois over \( \mathbb{Q} \), with \( \alpha_1(x) = x \) and \( \alpha_2(x) = -x \). Applying the theorem we have the following expression for \( \epsilon^{-1} f_T(T(x)) \).

\[
c(T(x))^3 f(x) f(-x) = \frac{8}{9} \cdot \frac{9x^6 - 262x^4 + 929x^2 - 100}{(x^2 + 1)^3}
\]

In order to write this as a polynomial in \( t \), we apply the recursive algorithm from above, taking \( \xi = 1 \) this time. We obtain the sequence of (ascending)
coefficients: 64, −96, −940/9, and 1300/9. After dividing the corresponding polynomial by its leading coefficient of 1300/9, we arrive at

\[
\begin{align*}
    f_T(t) &= t^3 - \frac{47}{325}t^2 - \frac{216}{325}t + \frac{144}{325} = (t - \frac{3}{5})(t + \frac{1}{5})(t - \frac{12}{13})
\end{align*}
\]

(which is correct).

3 An Example from Arithmetic Geometry

So far, our examples have involved degree two transformations that were clearly Galois in the sense of Definition 2.1. Moreover, in each case the conjugates of \(x\) were simply \(x\) and \(-x\). It is fair to ask whether there are naturally arising examples of higher degree and for which the Galois action is less immediate. One such family of examples arises in the context of arithmetic geometry, specifically in the study of elliptic curves. In fact, it was in this context that we first encountered the problem of applying Galois transformations to the roots of a polynomial (see [Mc, Remark 1.9]).

Recall that an elliptic curve \(E\) over a field \(K\) (with \(\text{char}(K) \neq 2\)) can be defined as a non-singular cubic equation of the form

\[
    E : \quad y^2 = x^3 + ax^2 + bx + c,
\]

where \(a, b, c \in K\) ([Si, §III.1]). The points of \(E\) over any fixed extension of \(K\) form an abelian group, with the infinite point serving as the group identity ([Si, §III.2]). For the purpose of this paper it is not necessary to review the group law for an elliptic curve, only the duplication rule. In particular, suppose that \(P = (x, y)\) is a point on \(E\). Then the \(x\) coordinate of the point \(2P\) is given by

\[
    x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4(x^3 + ax^2 + bx + c)}.
\]

So now suppose that the roots of some polynomial \(f(x)\) represent the \(x\) coordinates of some collection of points \(C\) on the elliptic curve \(E\) (perhaps the nontrivial points of a finite subgroup). As it turns out, the transformation defined by \(T(x) = x(2P)\) (from above) is always potentially Galois in the sense of Definition 2.1. Therefore, we can always use Theorem 2.5 to find the polynomial \(f_T(t)\), whose roots are the \(x\) coordinates of all of the points in \(\{2P | P \in C\}\). In short, we can double all of the points without actually finding them first!

In order to illustrate this with a concrete example, consider the elliptic curve \(E\) over the finite field \(\mathbb{F}_{43}\) defined by

\[
    y^2 = x^3 - 14x^2 - 6x + 17.
\]

Using the formula from above, we see that the duplication rule is

\[
    x(2P) = \frac{x^4 + 12x^2 + 36x + 42}{4(x^3 - 14x^2 - 6x + 17)}.
\]
Choose as the original polynomial,
\[ f(x) = (x + 4)(x - 8)(x + 9)(x - 15) = x^4 + 33x^3 + 29x^2 + x + 20. \]

Letting \( p \) and \( q \) be the numerator and denominator of \( T(x) := x(2P) \), we set \( h(X) = q(X)t - p(X) \). Note that \( c(t) \) is just \(-1\) in this case. One way to see that the extension is Galois is to substitute \( T(x) \) in for \( t \), and note that \( h(X) \) then completely factors as follows.
\[
\frac{-1(X - x)(xX - 2x - 2X + 11)(xX + 12x + 12X - 16)(xX + 19x + 19X - 1)}{(x - 2)(x + 12)(x + 19)}
\]
(In other words, \( h(X) \) splits over \( K(t)[x] \) where \( t = T(x) \).) Moreover, the roots of \( h(X) \), which are now evident, give us the four distinct conjugates of \( x \).
\[
\{\alpha_1(x), \alpha_2(x), \alpha_3(x), \alpha_4(x)\} = \left\{ \frac{2x - 11}{x - 2}, \frac{-12x + 16}{x + 12}, \frac{-19x + 1}{x + 19} \right\}
\]

Now we apply Theorem 2.5 by computing the norm of \( f(x) \).
\[
f(\alpha_1(x))f(\alpha_2(x))f(\alpha_3(x))f(\alpha_4(x)) = \frac{-18x^{16} - 17x^{15} + \cdots + 11x^2 - 19x}{x^{12} - 13x^{11} + \cdots - 6x + 15}
\]
This must be a constant multiple of \( f_T(T(x)) \). In order to deduce \( f_T(t) \), we choose a root, \( \xi \), of \( p(x) \) (which will lie in the quadratic extension of \( \mathbb{F}_{43} \)) and apply the recursive algorithm described in Section 2. For example, we may take \( \xi = 20 + 12\sqrt{2} \). After dividing the resulting polynomial by the leading coefficient, we have
\[
f_T(t) = t^4 + 8t^3 + 12t^2 + 39t + 9 = (t - 2)^2(t - 12)(t - 19).
\]

By applying \( T(x) \) to each of the four original roots, we see that this is correct.

**Remark 3.1.** One of the goals of our method was to avoid factoring, i.e., finding roots, but we did that twice in the previous calculation. First we substituted \( t = T(x) \) into \( h(X) \) and factored. Later, we chose \( \xi \) to be a root of \( p(x) \). Is this a problem? No. To be more precise about the goal, we seek an algorithm that does not require factoring the original \( f(x) \). Philosophically, this method will work well when the degree of the transformation, \( T(x) \), is small.

One last comment about this example is that it actually generalizes to multiplication by almost any integer on any elliptic curve.\(^3\) The issue of whether \( T(x) \) is potentially Galois boils down to this. If \( x \) is one root of \( h(X) \), i.e., if \( t = T(x) \), can all others roots then be written as functions of \( x \) alone? Well, when \( T(x) \) is the multiplication by \( n \) map (for \( x \) coordinates) on an elliptic curve, this will always be the case over a suitable extension \( L \). The reason is that we may alternatively compute the Galois conjugates of \( x \) by adding the

\(^3\)The one exception is when we multiply by an integer that is divisible by \( p = \text{char}(K) \).
generic point \((x, y)\) to each of the distinct \(n\)-torsion points on the curve (which must be defined over some finite extension \(L\) of \(K\)). In the previous example, this would mean adding \((x, y)\) to the three distinct points of order two: \((2, 0)\), \((-12, 0)\), and \((-19, 0)\). Omitting the details of the addition on \(E\), the results of adding these points are as follows.

\[
\begin{align*}
(x, y) + (2, 0) &= \left(\frac{2x - 11}{x - 2}, \ldots \right) \\
(x, y) + (-12, 0) &= \left(\frac{-12x + 16}{x + 12}, \ldots \right) \\
(x, y) + (-19, 0) &= \left(\frac{-19x + 1}{x + 19}, \ldots \right)
\end{align*}
\]

Note that this agrees with the conjugates of \(x\), as calculated above. This second method for finding the conjugates of \(x\) by adding explicit \(n\)-torsion points on \(E\), in order to apply the multiplication by \(n\) map to the roots, would admittedly require computing the \(n\)th torsion polynomial first. (For example, one could use [Si, Ex. 3.7].) However, we note again that the complexity would still depend on the degree of the transformation, rather than on the degree of the polynomial. This is a very important point.

4 Conclusion

The problem of applying a rational function, \(T(x)\), to the roots of a polynomial, \(f(x)\), without first finding the roots, is a very natural problem that could arise in any sort of computational algebra setting. The case where \(T(x)\) is invertible is well-understood and easy to solve. In theory, the completely general case could be handled by interpreting the coefficients of \(f(x)\) as elementary symmetric functions of the roots. However, the complexity of this approach depends greatly on the size of \(f\). In particular, it requires symbolic calculations in \(n\) variables, where \(n\) is the degree of \(f\). Somewhere in the middle lies the case where \(T(x)\) is a “Galois transformation” (Definition 2.1). In this case we have presented a very different algorithm, using elementary Galois theory of function fields, which appears to depend primarily on the degree of \(T\). It would be interesting to see a full complexity analysis of the algorithm, based on the degrees of both \(f\) and \(T\).

There are several other ways in which the ideas of this article could be further explored. One way would be to relax the (potentially) Galois hypothesis in the main theorem. When the extension fails to be normal, as is the case in Example 2.3, it may still be possible to (1) compute \(f_T(T(x))\) in terms of multiple roots of \(h(X)\) (as many as are necessary to split it), and then (2) infer \(f_T(t)\) as a polynomial in \(t\) alone. If the extension fails to be separable,\(^4\) it should be possible to reduce to the separable case by writing the irreducible polynomial as a separable polynomial in \(x^p\) (i.e., using the well-known result of [DF, §13.5, An example of this would be \(T(x) = x^p\), when \(K\) has characteristic \(p\) a prime.

\(^4\)An example of this would be \(T(x) = x^p\), when \(K\) has characteristic \(p\) a prime.
Prop 38], see also the proof of [La1, VII, Prop 4.3]). Finally, the equation $t = T(x)$ can be viewed as defining an algebraic map from $\mathbb{P}^1$ to $\mathbb{P}^1$ (as in Example 2.3). It would be interesting to see if our construction might have a more elegant presentation or interpretation in the language of algebraic curves.

References

(Note to Editor/Reviewer: Will update reference to 3rd edition.)

(Note to Editor/Reviewer: Will update reference to 3rd edition.)


(Note to Editor/Reviewer: This preprint will be available on arXiv soon.)
