NSERC USRA Report Summer 2017 Simplifying polynomials of degree 5 by Tschirnhaus Transformation

Student: Jinhui Li
Supervisor: Zinovy Reichstein

August 31, 2017

1 Introduction

This summer I worked on applying Tschirnhaus Transformation to the general polynomial of degree 5 using PGL_2-covariant and the computer program Maple with its extensional FGb package. Tschirnhaus Transformation is a type of nonlinear substitution on polynomials that is developed by Ehrenfried Walther von Tschirnhaus in 1683. Let f(x)=$x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_{n-1}x + a_n$ be a monic polynomial of degree n whose coefficients are algebraically independent over a base field k of characteristic 0. Let K=k($a_1, ...a_n$), let L=K[x]/f(x) be the root field of f over K, L/K is a finite separable field extension of degree n. Tschirnhaus Transformation is used to find a generating element y $\in L$ whose minimal polynomial g(y)=$y^n + b_1y^{n-1} + b_2y^{n-2} + ... + b_n$ over K is "simple". Let K_y=$k(b_1, b_2, ...b_n)$, "simple" here means to minimize the transcendence degree of K_y. For example, when n=2, p(x)=$x^2 + a_1x + a_2 = 0$, now let $y = x + a_1/2$ be the new generator for L/K. plug in x=y-$a_1/2$, we get q(y)=$y^2 + a_2 - a_1^2/2 = y^2 + b_2 = 0$. Then the transcendence degree of K_Y is 1, which is the minimum. I focused on the case of quintic polynomials, where n = 5. It is shown in [3] that a general polynomial of degree 5 can be reduced, via a Tschinrhaus transformation, to a polynomial with only two algebraically independent coefficients. The goal of my project was to come up with a constructive version of this proof, using a computer algebra system. My project thus involved three components: (i) learning standard background material in abstract algebra, mostly from Galois theory, (ii) familiarizing myself with contemporary research on Tschirnhaus transformations, in particular, reading research papers [1], [2] and [3], and adopting the methods from these papers to my problem, and (iii) carrying out computer calculations.

2 The Theorem

Theorem 1. *Let f(x)=x^5+a_1x^4+a_2x^3+...+a_2x+a_5 be a general polynomial of degree 5 whose coefficients are algebraically independent over a base field k of characteristic 0, then there exists a Tschirnhaus Transformation that is able to trasform the polynomial to the form $g(t) = t^5 + C_1t^4 + C_2t^3 + ...C_4t + C_5$, where $C_1, C_2, ...C_5$ satisfy the relations in U that is included in section 5 of this report, and $Trdeg_k k(C_1, C_2, C_3, C_4, C_5) = 2$.*

3 Main Theoretical Method

The rest of the report is dedicated to construct the proof of the theorem, which involves many related definitions, theorems, and technicalities. Let the base field with characteristic of 0 to be N. Suppose f(x)=$x^5 + a_1x^4 + a_2x^3 + ... + a_4x+a_5$ with $a_1, ...a_5$ algebraically independent over N. Let K=N(a_1, a_2, a_3, a_4, a_5), L=K[x]/f(x), M=$L^{norm} = N(x_1, x_2, x_3, x_4, x_5)$, where x_1, x_2, x_3, x_4, x_5 are distinct roots of f(x) and they are algebraically independent over N, it's clear that a_1, a_2, a_3, a_4, a_5 also represent the elementary symmetric polynomials of x_1, x_2, x_3, x_4, x_5. The roots are algebraically independent over N is by Corollary 18.8 in [4], Since K/N is a finitely generated field extension, and M/K is finite extension, hence $Trdeg_N M = Trdeg_N K = 5$. By the Fundamental theorem of Galois, M/K is a Galois extension with Galois group of S_5, M/L is a Galois extension with Galois group of S_4. And L/K is a field extension of degree 5, and there are no proper subfields between L and K. A new generator in L that is invariant under both S_4 and PGL_2 is needed for the Tschirnhaus Transformation. S_4 action is clear, it acts on the combinations of x_1, x_2, x_3, x_4, x_5, taken four at a time. PGL_2 acts on M as follows:

let the action g=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$,where a,b,c,d$\in N$, then $x_i^{'} = g(x_i)=\frac{ax_i+b}{cx_i+d}$, where $1 \leq i \leq 5$, then g sends the function $f(x_1, ...x_5)$ to $f(x_1^{'}, ...x_5^{'})$. This action commutes with the S_5-action and hence, descends to L.

Since $L \cong K(x_1) \cong K(x_2) \cong K(x_3) \cong K(x_4) \cong K(x_5)$ by the first Isomorphism theorem, A new generator in L also means new generators in $K(x_1), K(x_2), K(x_3), K(x_4)$, and $K(x_5)$. Let J_1, J_2, J_3, J_4, J_5 denote the new generators in $K(x_1), K(x_2), K(x_3), K(x_4), and\, K(x_5)$ respectively. Since K(x_i),where $1 \leq i \leq 5$, is invariant under S_4, meaning that it includes all the functions with coefficients in N of variable $x_1, ...x_{i-1}, x_{i+1}, ...x_5$ that are invariant when S_4 acts on $x_1, ...x_{i-1}, x_{i+1}, ...x_5$. Hence in order to make it easier to construct such generator, J_1 is set to be the function of x_2, x_3, x_4, x_5 and since Tschirnhaus Transformation applies to every generator equally, hence $J_2 = (12)J_1, J_3 = (13)J_1$,$J_4 = (14)J_1, J_5 = (15)J_1$. Hence applying Tschirnhaus Transformation to J_1 and make it invariant under under both S_4 and PGL_2 will also set the other four generators to have the same properties. Representing J_1 in terms of the cross-ratio of x_2, x_3, x_4, x_5 is a way to guarantee the J_1 is invariant under PGL_2 which means $J_1(x_2, x_3, x_4, x_5) = J_1((ax_2 + b)/(cx_2 + d), (ax_3 +$

$b)/(cx_3+d), (ax_4+b)/(cx_4+d), (ax_5+b)/(cx_5+d))$, where a,b,c,d$\in N$. So let $k_1 = [x_2, x_3, x_4, x_5]$=$(x_4-x_2)(x_5-x_3)/(x_4-x_3)(x_5-x_2)$, and S_4 acts on k_1 as $\sigma(k_1) = (x_{\sigma(4)}-x_{\sigma(2)})(x_{\sigma(5)}-x_{\sigma(3)})/(x_{\sigma(4)}-x_{\sigma(3)})(x_{\sigma(5)}-x_{\sigma(2)})$. Four points x_2, x_3, x_4, x_5 have 24 ways to be ordered, but there are only six ways to partition them into two non-ordered pairs, hence four points have six different cross-ratios which are all related. They are $k_1, 1/k_1, 1-k_1, 1/(1-k_1), (k_1-1)/k_1, k_1/(k_1-1)$. Let g$(k_1) = 1/k_1\, and\, h(k_1) = 1-k_1$, Since $1/(1-k_1) = g\circ h(k_1), (k_1-1)/k_1 = h\circ g(k_1), k_1/(k_1-1) = g\circ(h\circ g(k_1))$. If J_1 is a function of k_1 that is invariant under the functions of g$(k_1) = 1/k_1$ and $h(k_1) = 1-k_1$, then it is invariant under any permutation of S_4 acting on k_1. By some luck, I found that the function $J_1 = (k_1^2-k_1+1)^3/(k_1^2*(k_1-1)^2)$ is the function we need. Because

$J_1\circ g(k_1) = (1/k_1^2-1/k_1+1)^3/(1/k_1^2*(1/k_1-1)^2) = ((k_1^2-k_1+1)^3/k_1^6)/((k_1^2-2k_1+1)/k_1^4) = (k_1^2-k_1+1)^3/((k_1-1)^2k_1^2) = J_1(k_1)$

Similarly, $J_1\circ h(k_1) = ((1-k_1)^2-(1-k_1)+1)^3/((1-k_1)^2*(1-k_1-1)^2) = (k_1^2-k_1+1)^3/((1-k_1)^2k_1^2) = J_1(k_1)$.

There are also several other J-invariants that can be used as the generators, for example,

$J_1^* = k_1^2+(1-k_1)^2+1/k_1^2+1/(1-k_1)^2+((k_1-1)/k_1)^2+(k_1/(k_1-1))^2 = (2{k_1}^6-6k_1^5+9k_1^4-8k_1^3+9*k_1^2-6*k_1+2)/(k_1^2(k_1-1)^2)$,

but J_1 gives a more concise result in the end. After we determine the J_1, we plug it in $J_2 = (12)J_1, J_3 = (13)J_1$,$J_4 = (14)J_1$,$J_5 = (15)J_1$, notice that J_2, J_3, J_4, J_5 will be the functions of the variable of k_2, k_3, k_4, k_5 respectively, where k_2, k_3, k_4, k_5 are cross-ratios such that $k_2 = (12)k_1, k_3 = (13)k_1, k_4 = (14)k_1, k_5 = (15)k_1$. J_1, J_2, J_3, J_4, J_5 are the generators of $K^*(J_1), K^*(J_2), K^*(J_3), K^*(J_4), K^*(J_5)$ respectively which are all isomorphic to $L^* = K^*[J]/g(J)$, where $g(J)$= $J^5+C_1J^4+C_2J^3+C_3J^2+C_4J+C_5$, K^* is the subfield of K that is invariant under PGL_2. Notice that C_1, C_2, C_3, C_4, C_5 are the elementary symmetric polynomials of J_1, J_2, J_3, J_4, J_5, namely

$C_1 = -(J_1+J_2+J_3+J_4+J_5), C_2 = J_1J_2+J_1J_3+J_1J_4+J_1J_5+J_2J_3+J_2J_4+J_2J_5+J_3J_4+J_3J_5+J_4J_5, C_3 = -(J_1J_2J_3+J_1J_2J_4+J_1J_2J_5+J_1J_3J_4+J_1J_3J_5+J_1J_4J_5+J_2J_3J_4+J_2J_3J_5+J_2J_4J_5+J_3J_4J_5), C_4 = J_1J_2J_3J_4+J_1J_2J_4J_5+J_1J_2J_3J_5+J_1J_3J_4J_5+J_2J_3J_4J_5, C_5 = -J_1J_2J_3J_4J_5$.

Let M^* be the subfield of M invariant under PGL_2, hence $M^* = M^{PGL_2} = N(J_1, J_2, J_3, J_4, J_5)$, then $K^* = (M^*)^{S_5} = N(C_1, C_2, C_3, C_4, C_5)$. Hence M^*/K^* and M^*/L^* are Galois extensions with Galois group S_5 and S_4 respectively. Our original plan was to find the three independent polynomial relations among C_1, C_2, C_3, C_4, C_5, and in order to do that, we have to find the three independent relations among J_1, J_2, J_3, J_4, J_5 first. all of these relations exist because PGL_2-covariant condition makes the transcendence degree of M^*, L^*, and K^* to be 2. However, any set of relations that generates the polynomial ideal that contains the polynomial ideal that is generated by the three independent relations also makes the transcendence degree of K^* to be 2, which is what included in the theorem.

4 Computer Algebra Methods

I will discuss the main computer algebra methods in this section, the main result will be discussed in next section. A computer algebra program with strong functionalities is needed in order to find the independent polynomial relations due to the high degree polynomials in both the denominator and the numerator of the J-invariants.initially I tried basically all the related and built-in functionalities in both Maple and Mathematica, but they failed to do the job. Luckily I found that an extensional Maple package online called FGb that is able to find the relations. FGb is a fast library for computing Grobner bases which in our case is a particular kind of generating set of the ideal I in the polynomial ring $N[k_1, k_2, k_3, k_4, k_5, J_1, J_2, J_3, J_4, J_5]$. Here I is the ideal generated by the polynomial relations among $k_1, k_2, k_3, k_4, k_5, J_1, J_2, J_3, J_4, J_5$ after normalizing the J-invariants. By the definitions of J_1, J_2, J_3, J_4, J_5, we already have five polynomial relations. We need three more independent relations among k_1, k_2, k_3, k_4, k_5 in order to obtain three independent relations among J_1, J_2, J_3, J_4, J_5, which exists in principle since PGL_2-covariant makes the transcendence degree of $N(k_1, k_2, k_3, k_4, k_5)$ to be 2 as well. By some simple computation and verifying on Maple, the three independent relations are: $k_2k_3 = k_1, k_4k_5 = k_1, (1 - k_2) * (1 - k_4) = 1 - k_1$. Hence

$I = (k1^2 * (k1 - 1)^2 * J1 - (k1^2 - k1 + 1)^3, k2^2 * (k2 - 1)^2 * J2 - (k2^2 - k2 + 1)^3, k3^2 * (k3 - 1)^2 * J3 - (k3^2 - k3 + 1)^3, k4^2 * (k4 - 1)^2 * J4 - (k4^2 - k4 + 1)^3, k5^2 * (k5 - 1)^2 * J5 - (k5^2 - k5 + 1)^3, k2 * k3 - k1, k4 * k5 - k1, (1 - k2) * (1 - k4) - 1 + k1)$,

notice that all the subscripts are omitted since they are copied from Maple. Now the line $fgb\_gbasis\_elim(I, 0, [k1, k2, k3, k4, k5], [J1, J2, J3, J4, J5])$ will output the generators of I that is solely dependent on J_1, J_2, J_3, J_4, J_5. Here 0 represents the field of characteristic of 0. Denote the new generating sets of I that is solely in terms of J_1, J_2, J_3, J_4, J_5 to be R. Now let H denote the new ideal generated by R and the elementary symmetric polynomials of J_1, J_2, J_3, J_4, J_5. hence

$H = (C1 + (J1 + J2 + J3 + J4 + J5), C2 - (J1 * J2 + J1 * J3 + J1 * J4 + J1 * J5 + J2 * J3 + J2 * J4 + J2 * J5 + J3 * J4 + J3 * J5 + J4 * J5), C3 + (J1 * J2 * J3 + J1 * J2 * J4 + J1 * J2 * J5 + J1 * J3 * J4 + J1 * J3 * J5 + J1 * J4 * J5 + J2 * J3 * J4 + J2 * J3 * J5 + J2 * J4 * J5 + J3 * J4 * J5), C4 - (J1 * J2 * J3 * J4 + J1 * J3 * J4 * J5 + J1 * J2 * J4 * J5 + J1 * J2 * J3 * J5 + J2 * J3 * J4 * J5), C5 + J1 * J2 * J3 * J4 * J5, R)$.

Then the line $fgb\_gbasis\_elim(H, 0, [J1, J2, J3, J4, J5], [C1, C2, C3, C4, C5])$ is able to output the new generating setsof H that is solely depend on C_1, C_2, C_3, C_4, C_5, denote it U.

5 Main Result and Discussion

From previous section, relations in R and U contain the most concise relations that I could obtain within the time limit of this research and everyone of them has been verified to be correct. As mentioned in the section 3, originally, we expected to see three independent relations in both R and U. But in reality, the program gave us 13 relations in R, and 11 relations in U. Since the relations in R are just the stepstone for getting relations in U, hence only the relations in U is included in this report:

$U = \{-18225216*C1*C3*C5^2+113038400*C1*C4*C5^2+38234624*C1*C5^3+12363840*C2*C3*C4*C5-14928192*C2*C3*C5^2+2286208*C2*C4*C5^2-5508608*C2*C5^3-5427200*C3^2*C5^2+881920*C3*C4^2*C5+2754304*C3*C4*C5^2+118720*C4^4-688576*C4^3*C5+3422379600*C1*C3*C5-10318100208*C1*C4*C5-13463482304*C1*C5^2-98910720*C2*C3*C4+208445184*C2*C3*C5+1880727472*C2*C4*C5-294018560*C2*C5^2-148824000*C3^2*C5-33886080*C3*C4^2-412894592*C3*C4*C5-561806784*C3*C5^2-7455616*C4^3+129435328*C4^2*C5+1356579520*C4*C5^2+833482240*C5^3-65001738551*C1*C3-948113500463*C1*C4-2377460148132*C1*C5+261320544989*C2^2+6557780736*C2*C3+142510973211*C2*C4+92954235288*C2*C5-61819200*C3^2+4337967744*C3*C4-75429917152*C3*C5+20701762052*C4^2-111745986944*C4*C5-89658291216*C5^2-59726498761800*C1-723900019740*C2-719895170440*C3-7210994658460*C4-23505852782913*C5-582413878748480=0,$

$53*C2^3-603*C1*C3+5459*C1*C4+1272*C1*C5-2380*C2^2+477*C2*C3+371*C2*C4-424*C2*C5+212*C3*C4+141472*C1+17968*C2-13160*C3+35000*C4+22697*C5+1351936=0,$

$1321184*C1*C3*C5+10021664*C1*C4*C5+4355328*C1*C5^2+2163672*C2^2*C3+1236384*C2*C3*C4-1236384*C2*C3*C5+247616*C2*C4*C5-474880*C2*C5^2-732672*C3^2*C5+183168*C3*C4^2+237440*C3*C4*C5-59360*C4^3-193883881*C1*C3-1860695857*C1*C4-3389650828*C1*C5+615051451*C2^2-50382648*C2*C3+371171349*C2*C4-56205864*C2*C5-309096*C3^2-11127456*C3*C4-140867216*C3*C5+59336044*C4^2+130054368*C4*C5+110511360*C5^2-114549969960*C1-5704279788*C2-1527020288*C3-15992191092*C4-28477757215*C5-1075766900800=0,$

$8654688*C1*C3^2+1321184*C1*C3*C5+10021664*C1*C4*C5+4355328*C1*C5^2+1236384*C2*C3*C4-1236384*C2*C3*C5+247616*C2*C4*C5-474880*C2*C5^2-732672*C3^2*C5+183168*C3*C4^2+237440*C3*C4*C5-59360*C4^3+469281587*C1*C3-1803358549*C1*C4-3848349292*C1*C5+375965695*C2^2-4945536*C2*C3+313834041*C2*C4-56205864*C2*C5+75419424*C3^2-19782144*C3*C4-123557840*C3*C5+59336044*C4^2+130054368*C4*C5+110511360*C5^2-72206908920*C1-2002236996*C2+4117999960*C3-16260486420*C4-37172473147*C5-703372985536=0,$

$388384*C1*C3*C5+296800*C1*C4*C5+40704*C1*C5^2+57240*C2^2*C4-45792*C2*C3*C5-3392*C2*C4*C5-13568*C2*C5^2+6784*C3*C4*C5-1696*C4^3+3469873*C1*C3-61098983*C1*C4-62363828*C1*C5+12058397*C2^2-1236384*C2*C3+5536539*C2*C4+3064248*C2*C5-538056*C3*C4+1735856*C3*C5+1345988*C4^2+3383520*C4*C5+1221120*C5^2-2998850040*C1-3506820*C2+49775408*C3-469697676*C4-635036057*C5-29486572736=0,$

$228960*C1*C3*C4+388384*C1*C3*C5+296800*C1*C4*C5+40704*C1*C5^2-45792*C2*C3*C5-3392*C2*C4*C5-13568*C2*C5^2+6784*C3*C4*C5-1696*C4^3+8735953*C1*C3-27899783*C1*C4-44161508*C1*C5+10741877*C2^2-1236384*C2*C3+6738579*C2*C4-3003192*C2*C5+1465344*C3*C4+1735856*C3*C5+1117028*C4^2+3841440*C4*C5+1221120*C5^2-1743805800*C1-139680780*C2+95853608*C3-260313756*C4-302929577*C5-15867116096=0,$

$-6784*C1*C3*C5+1696*C1*C4^2+6467*C1*C3+1115067*C1*C4+1641940*C1*C5-290321*C2^2-184599*C2*C4-8904*C2*C5+22896*C3*$

$C5 - 17172 * C4^2 - 3392 * C4 * C5 - 13568 * C5^2 + 60859144 * C1 + 1610556 * C2 + 91288 * C3 + 9308972 * C4 + 15159221 * C5 + 585392960 = 0$,

$-160272 * C1 * C3 * C5 - 114480 * C1 * C4 * C5 - 20352 * C1 * C5^2 + 5936 * C2 * C3 * C5 + 4240 * C2 * C4^2 + 1696 * C2 * C4 * C5 + 6784 * C2 * C5^2 - 3392 * C3 * C4 * C5 + 848 * C4^3 - 345009 * C1 * C3 + 23763239 * C1 * C4 + 32588004 * C1 * C5 - 6096741 * C2^2 + 160272 * C2 * C3 - 3635747 * C2 * C4 - 394744 * C2 * C5 + 68688 * C3 * C4 + 88192 * C3 * C5 - 652324 * C4^2 - 1144800 * C4 * C5 - 644480 * C5^2 + 1339684840 * C1 + 25509580 * C2 - 4997544 * C3 + 191021148 * C4 + 306730281 * C5 + 12970376768 = 0$,

$-64 * C1 * C3 * C5 + 16 * C2^2 * C5 + 227 * C1 * C3 + 9275 * C1 * C4 + 16372 * C1 * C5 - 2561 * C2^2 - 1431 * C2 * C4 - 760 * C2 * C5 + 288 * C3 * C5 - 212 * C4^2 + 64 * C4 * C5 - 128 * C5^2 + 570600 * C1 + 9420 * C2 + 2344 * C3 + 72012 * C4 + 160245 * C5 + 5539392 = 0$,

$106 * C1^2 + 4 * C1 * C3 - C2^2 + 1958 * C1 + 21 * C2 + 35 * C3 - 4 * C4 + 8 * C5 + 8944 = 0$,

$106 * C1 * C2 + 12 * C1 * C3 - 3 * C2^2 - 3242 * C1 + 1229 * C2 + 105 * C3 + 94 * C4 + 24 * C5 - 32528 = 0\}$.

It would be the best to find the sub ideal in U that is generated by the three independent relations of C_1, C_2, C_3, C_4, C_5, but due to the time limit of this research and my limited knowledge of computer algebra, such ideal is not found. Nevertheless, since U generate H entirely, the relations in U are capable of reducing the Transcendence degree of K^* by 3, hence this completes the constructive proof of the theorem.

6 Acknowledgement

I would like to thank NSERC for funding the project, Prof. Zinovy Reichstein for his excellent supervision and patient guidance, and Dr. Uriya First for his helpful lessons about Galois Theory.

References

[1] Buhler, J., & Reichstein, Z. (1999). On Tschirnhaus Transformations. Topics in Number Theory, 127-142. doi:10.1007/978-1-4613-0305-3_7

[2] Kraft, H. (2006). A result of Hermite and equations of degree 5 and 6. Journal of Algebra, 297(1), 234-253. doi:10.1016/j.jalgebra.2005.04.015

[3] Reichstein, Z., & Buhler, J. (1997). On the essential dimension of a finite group. Compositio Mathematica, 106, 159-179. doi:10.1023/A:1000144403695

[4] Stewart, I. (2015). Galois theory. Boca Raton: Chapman & Hall/CRC.

[5] Ehrenborg, R., & Rota, G. (1993). Apolarity and Canonical Forms for Homogeneous Polynomials. European Journal of Combinatorics, 14(3), 157-181. doi:10.1006/eujc.1993.1022

[6] Dummit, D. S., & Foote, R. M. (1991). Abstract algebra. Englewood Cliffs, N.J.: Prentice Hall.