University of Luxembourg

Master in Mathematics

Galois groups in generalisation of Maeda's conjecture

Galois theory and polynomials with symmetric Galois groups

Author: Valnea Skansi

Supervisors: G. Wiese and P. Tsaknias

December 2014

Contents

1 Introduction

The main focus of the work before you is Galois theory, named after Évariste Galois - a French mathematician who lived in the beginning of the $19th$ century. In its essence, Galois theory connects field theory and group theory, and so the contents will be structured in such a way as well. We shall begin with a short overview of field theory, followed by the the basics of Galois theory such as definitions and important theorems.

The goal of this thesis is the disprovement or the experimental verification of the second part of Maeda's conjecture that says that the Galois group of the coefficient field of certain modular forms is the symmetric group (of degree of the field dimension). This topic is in fact shared between me and my colleague, Lucija Calic, with her work focusing mostly on modular forms and the presentation of the conjecture itself.

We will try to provide a theoretical foundation for the question at hand by focusing on how to view the Galois group of a polynomial as a permutation group on the roots of the polynomial, and particularly how the factorisation types of polynomials give information on cycles in the Galois group.

Once we have established that the Galois group in question is a transitive subgroup of the symmetric group, we will make a small digression towards group theory and examine various criteria that can be used to deduce the opposite inclusion.

Finally, we will present the code and the computational results, made in collaboration with L.Calic. They will be obtained using Sage, and with it we shall test the above mentioned second point of Maeda's conjenture.The primary focus will be on the the squarefree levels.

2 Basics of Galois theory

2.1 Field Theory

We shall begin by revising some of the definition on fields, field theory and field extensions, mostly following the setup from [2] but also other sources.

Definition 2.1. $\mathbf{F}$ is a *field* with respect to multiplication and addition if there exist distinct neutral element for $+$ and $\cdot$, $+$ and $\cdot$ are closed, associative and commutative operations, every element has an inverse with respect to $+$ and every nonzero has an inverse with respect to $\cdot$, and furthermore, if multiplication is distributive over addition.

For p a prime, $\mathbf{F}_p = \{0,\ 1,\ ...,\ p-1\}$ with addition and multiplication defined modulo p is a field.

Definition 2.2. An *integral domain* is a nonzero commutative ring where zero is the only zero diviser.

Definition 2.3. A *unique factorization domain* (UFD) is a commutative ring such that every non-zero non-unit element can be written as a product of prime elements (or irreducible elements), uniquely up to order and units.

For any field $\mathbf{F}$, we let $\mathbf{F}[X]$ be the ring of polynomials in the variable X with coefficients in $\mathbf{F}$, i.e. $f \in \mathbf{F}[X] \Rightarrow f = a_0 + a_1X + a_2X^2 + ... + a_nX^n$ where $a_i \in \mathbf{F}$.

Let us now take $f(X) \in \mathbf{F}[X]$. We consider *(principal) ideal* $< f(X) >$ generated by $f(X)$, i.e. the set of all multiples (by polynomials) of $f(X)$. Then we can form a *quotient ring* $\mathbf{F}[X]/ < f(X) >$, by setting the multiples of $f(X)$ to be equal to zero. The following proposition tells us when that quotient ring is a field.

Proposition 2.4. *Let $f(X) \in \boldsymbol{F}[X]$ be an irreducible poynomial of degree d. Then $\boldsymbol{F}[X]/ < f(X) >$ is a field and a d-dimensional $\boldsymbol{F}$-vector space.*

Definition 2.5. A field $\mathbf{L}$ is an *extension* of $\mathbf{K}$ if $\mathbf{K} \subseteq \mathbf{L}$ and $\mathbf{K}$ is also a field. We use the notation: $\mathbf{L}/\mathbf{K}$

If $\mathbf{L}$ is an extension of $\mathbf{F}$ which is in turn an extension of $\mathbf{K}$, then $\mathbf{F}$ is said to be an *intermediate field* or *intermediate extension* of the field extension $\mathbf{L}/\mathbf{K}$. For example, the field of complex numbers $\mathbb{C}$ is an extension field of the field of real numbers $\mathbb{R}$, and $\mathbb{R}$ is an extension field of the field of rational numbers $\mathbb{Q}$. It is clear that $\mathbb{C}/\mathbb{Q}$ is also a field extension.

Definition 2.6.
(1) The *degree* of $\mathbf{L}$ over $\mathbf{K}$ is the dimension of $\mathbf{L}$ seen as a $\mathbf{K}$-vector space. We use the notation $(\mathbf{L} : \mathbf{K})$.
(2) $\mathbf{L}$ is a *finite* extension of $\mathbf{K}$ (or $\mathbf{L}/\mathbf{K}$ is *finite*) if $(\mathbf{L} : \mathbf{K})$ is finite.

For example, let us take a look at $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})$. $\mathbb{Q}(\sqrt{3}) = \{a+b\sqrt{3} : a, b \in \mathbb{Q}\}$. Obviously, the dimension of $\mathbb{Q}(\sqrt{3})$ seen as a $\mathbb{Q}$-vector space is two. So by definition, the dimension of the field extension is $(\mathbb{Q}(\sqrt{3}) : \mathbb{Q}) = 2$.

Definition 2.7.
(1) Let $\mathbf{L}$ be an extension of $\mathbf{K}$. Then $\alpha \in \mathbf{L}$ is *algebraic* over $\mathbf{K}$ if α is a root of some polynomial $f(x) \in \mathbf{K}[X]$.
(2) $\mathbf{L}$ is an *algebraic extension* of $\mathbf{K}$ if every $\alpha \in \mathbf{L}$ is algebraic over $\mathbf{K}$.

Definition 2.8.
(1) Let $f\ (X) \in \mathbf{K}[X]$ be a non-constant polynomial. If $\mathbf{K} \subseteq \mathbf{L}$ is such that $f(X)$ factors into (possibly repeated) linear factors in $\mathbf{L}[X]$, then $f(X)$ *splits* in $\mathbf{L}[X]$, i.e. $f(X)$ *splits* in $\mathbf{L}[X]$ if we can write polynomial $f(X) \in \mathbf{K}[X]$ as

$$f(X) = \prod_{i=1}^{\deg(f)} (X - a_i) \in \mathbf{L}[X]$$

where a_i for $i \in \{1, 2, ..., deg(f)\}$ generate the field extension $\mathbf{L}/\mathbf{K}$.

(2) If $f(X)$ splits in $\mathbf{L}[X]$ but not in $\mathbf{B}[X]$ for any subfield $\mathbf{B} \subset \mathbf{L}$, then $\mathbf{L}$ is a *splitting field* of $f(X)$, meaning that the extension $\mathbf{L}$ is an extension of minimal degree over $\mathbf{K}$ in which $f(X)$ splits.

Lemma 2.9. *Let $f(x) \in \boldsymbol{K}[X]$ be a polynomial, with $deg(f) = n > 0$. Then $f(X)$ has a splitting field $\boldsymbol{L}$, and $(\mathbf{L} : \mathbf{K}) \leq n!$*

Definition 2.10. An algebraic extension $\mathbf{L}$ of $\mathbf{K}$ is called a *normal* extension if every irreducible polynomial $f(X) \in \mathbf{K}[X]$ with a root in $\mathbf{L}$ splits into linear factors in $\mathbf{L}[X]$.

For example, algebraic closure $\mathbf{K_L}$ of a field $\mathbf{K}$ is a normal extension of $\mathbf{K}$.

Definition 2.11. Let $\mathbf{L}/\mathbf{K}$ be a field extension and let $\alpha \in \mathbf{L}$. The *minimal polynomial* of α is a monic polynomial of the smallest degree among all polynomials in $\mathbf{K}[X]$ that have α as a root. It is denoted as m_α.

Note: when the field extension $\mathbf{L}/\mathbf{K}$ is algebraic, minimal polynomial always exists.

Definition 2.12.
(1) If the irreducible factors of $f(X) \in \mathbf{K}[X]$ split into a product of distinct linear factors in a splitting field for $f(X)$ (meaning that all roots are distinct), then $f(X)$ is a *separable* polynomial. Otherwise, it is called *inseparable*.
(2) Let $\mathbf{L}$ be an algebraic extension of $\mathbf{K}$. $\alpha \in \mathbf{L}$ is a *separable* element if $m_\alpha(X)$ is a separable polynomial. Otherwise, α is an *inseparable* element.
(3) Let $\mathbf{L}$ be an algebraic extension of $\mathbf{K}$. Then $\mathbf{L}$ is a *separable* extension of $\mathbf{K}$ if every $\alpha \in \mathbf{L}$ is a separable element. Otherwise, it is an *inseparable* extension.

For example, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a separable extension because the minimal polynomal of $a + b\sqrt{2}$ when $b \neq 0$ is $X^2 - 2aX + a^2 - 2b^2 = (X - a + b\sqrt{2})(X - a - b\sqrt{2})$

2.2 Galois Theory

After having revised the fundamentals in the previous chapter, we are now able to focus on what interests us the most - *Galois extensions* and a *Galois groups*.

Definition 2.13. The symmetric group S_n of degree n is the group of all permutations on n symbols.

Definition 2.14. Let G be a group of automorphisms of a field $\mathbf{K}$. Then we define *fixed field* as $\mathrm{Fix}(G) := \{\alpha \in \mathbf{K} \mid \sigma(\alpha) = \alpha \ for\ all\ \sigma \in G\}$.

Definition 2.15. Let $\mathbf{L}$ be an algebraic extension of $\mathbf{K}$. The *Galois group* $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ is a group of all automorphism of $\mathbf{L}$ that restrict to the identity on $\mathbf{K}$, i.e. $\mathrm{Gal}(\mathbf{L}/\mathbf{K}) = \{\sigma : \mathbf{L} \to \mathbf{L}\ automorphism \mid \sigma_{|K} = id\}$, with respect to composition.

Let us quickly show Galois group is indeed, a group. Suppose f and g are $\mathbf{K}$-automorphisms of $\mathbf{L}$. Then $f \circ g$ is an automorphism. Furthermore, if $k \in \mathbf{K}$, then $f \circ g(k) = f(k) = k$ so we showed that $f \circ g$ is a $\mathbf{K}$-automorphism. The identity on $\mathbf{L}$ is clearly a $\mathbf{K}$-automorphism. Finally, f^{-1} is an automorphism of $\mathbf{L}$, and for any $k \in \mathbf{K}$, we have $k = f^{-1} \circ f(k) = f^{-1}(k)$ so that f^{-1} is a K-automorphism, and we know that composition of maps is associative.

Definition 2.16. Let $\mathbf{L}$ be an algebraic extension of $\mathbf{K}$. Then $\mathbf{L}$ is a *Galois extension* of $\mathbf{K}$ if $\mathrm{Fix}(\mathrm{Gal}(\mathbf{L}/\mathbf{K})) = \mathbf{K}$.

From the definition of a fixed field and Galois group we know that $\mathbf{K} \subseteq \mathrm{Fix}(\mathrm{Gal}(\mathbf{L}/\mathbf{K}))$, so if $\mathbf{L}$ is a Galois extension, it simply means that there

does not exist $\alpha \in \mathbf{L}\backslash\mathbf{K}$ such that $\forall\sigma \in Gal(\mathbf{L}/\mathbf{K})\ \sigma(\alpha) = \alpha$, i.e. all other elements of $\mathbf{L}$ which are not at the same time in $\mathbf{K}$ permute for some $\sigma \in$ Gal($\mathbf{L}/\mathbf{K}$).

There are several equivalent definitions of Galois extension, as we can see from the following theorem.

Theorem 2.17. *Let $\boldsymbol{L}$ be a finite extension of $\boldsymbol{K}$. The following statements are equivalent:*
(1) $\boldsymbol{L}$ is a Galois extension of $\boldsymbol{K}$.
(2) $\boldsymbol{L}$ is a normal and separable extension of $\boldsymbol{K}$.
(3) $\boldsymbol{L}$ is the splitting field of a separable polynomial $f(X) \in \boldsymbol{K}[X]$.

Theorem 2.18. ***(Fundamental theorem of Galois theory)***
Let $\boldsymbol{L}$ be a finite Galois extension of $\boldsymbol{K}$ and let $G = Gal(\boldsymbol{L}/\boldsymbol{K})$.
(1) There is a one-to-one correspondence between intermediate fields $\boldsymbol{L} \supseteq \boldsymbol{B} \supseteq \boldsymbol{K}$ and subgroups $\{1\} \subseteq G_{\boldsymbol{B}} \subseteq G$ given by $\boldsymbol{B} = Fix(G_{\boldsymbol{B}})$.
(2) $\boldsymbol{B}$ is a normal field extension of $\boldsymbol{K}$ if and only if $G_{\boldsymbol{B}}$ is a normal subgroup of G. This is the case if and only if $\boldsymbol{B}$ is a Galois extension of $\boldsymbol{K}$. In this case $Gal(\boldsymbol{B}/\boldsymbol{K}) \cong G/G_{\boldsymbol{B}}$.
(3) For each $\boldsymbol{L} \supseteq \boldsymbol{B} \supseteq \boldsymbol{K}$, $(\boldsymbol{B}/\boldsymbol{K}) = [G : Gal(\boldsymbol{L}/\boldsymbol{B})]$ and $(\boldsymbol{K}/\boldsymbol{B}) =\mid Gal(\boldsymbol{L}/\boldsymbol{B}) \mid$

Note: $G_{\boldsymbol{B}} = Gal(\boldsymbol{L}/\boldsymbol{B})$

Definition 2.19. Let $\mathbf{L}$ be an algebraic extension of $\mathbf{K}$, and let $\alpha \in \mathbf{L}$. Then $\{\sigma(\alpha) \mid \sigma \in \text{Gal}(\mathbf{L}/\mathbf{K})\}$ is the set of *(Galois) conjugates* of $\alpha \in \mathbf{L}$

Lemma 2.20. *Let $\boldsymbol{L}$ be a Galois extension of $\boldsymbol{K}$, and let $\alpha \in \boldsymbol{L}$. Then α has finitely many conjugates in $\boldsymbol{L}$. If we let $\{\alpha_i\}$, for $i \in \{1, 2, ..., r\}$ be the set of conjugates of $\alpha = \alpha_1$, then*

$$m_\alpha(X) = \prod_i^r (X - \alpha_i)$$

Lemma 2.21. *The multiplicative group of the Galois field is cyclic.*

The proofs of some of the above results have been purposely left out, but they can be found in [2], [5] or in any other book on Galois theory. This concludes the general definitions and theorems of Galois theory.

3 Galois group of a polynomial

Now we shall look at the Galois group of a polynomial.

3.1 Irreducibility ⇒ transitivity of the Galois group

We would like to show that we can see the Galois group as a permutation group on the roots. In particular, we would like to show that the Galois group of a polynomial is a transitive subgroup of the symmetric group if the polynomial is irreducible. In order to prove that, we first need the following two lemmas.

Definition 3.1. A non-constant polynomial $f(X) \in \mathbf{K}[X]$ is said to be *irreducible* over the field $\mathbf{K}[X]$ if $f(X)$ has a positive degree and if $f(X) = g(X)h(X)$, with $g(X),\ h(X) \in \mathbf{K}[X]$ implies that either $h(X)$ or $g(X)$ is a constant polynomial.

Definition 3.2. A permutation group (Σ, A) such that for any two elements $a_i, a_j \in A$ there exists $\sigma \in \Sigma$ such that $\sigma(a_i) = a_j$ is called a *transitive* permutation group.

Lemma 3.3. *Let $\sigma_0 : \boldsymbol{K}_1 \to \boldsymbol{K}_2$ be an isomorphism of fields. Let $f_1(X) \in \boldsymbol{K}_1[X]$ be irreducible and let $\boldsymbol{L}_1 = \boldsymbol{K}_1(\beta_1)$, where $f_1(\beta_1) = 0$. Let $f_2(X) = \sigma_0(f_1(X))$ and let $\boldsymbol{L}_2 = \boldsymbol{K}_2(\beta_2)$ where $f_2(\beta_2) = 0$. Then σ_0 extends to a unique isomorphism $\sigma : \boldsymbol{L}_1 \to \boldsymbol{L}_2$ with $\sigma(\beta_1) = \beta_2$.*

Proof.
We can see that if $f_1(X)$ is irreducible then $f_2(X)$ is also irreducible and vice versa, because σ_0 is an isomorphism: if $f_1(X)$ was reducible it could be written as $f_1(X) = g(X)h(X)$, where $h(X)$ or $g(X)$ are both non-constant polynomials in $\mathbf{K}_1[X]$. If we would then apply the isomorphism σ_0 to all coefficients of $f_1(X) = g(X)h(X)$, we would obtain $f_2(X) = g'(X)h'(X)$ in $\mathbf{K}_2[X]$, with $g'(X)$ and $h'(X)$ non-constant polynomials, so we have showed that the polynomial $f_2(X)$ is also reducible. Using similar steps and replacing σ_0 with σ_0^{-1} we can prove the converse.

If we have an element $\alpha \in \mathbf{L}$ that is algebraic over $\mathbf{K}$, we can define its minimal polynomial m_α. We now continue and define

$$\phi : \mathbf{K}[X] \to \mathbf{L}$$

a ring homomorphism, such that on the elements of $\mathbf{K}$, ϕ acts as an identity, and for non-constant elements we have: $\phi(f(X)) = f(\alpha)$.
In turn, ϕ induces an isomorphism

$$\tilde{\phi} : \mathbf{K}[X]/ < m_\alpha(X) > \to \mathbf{K}(\alpha)$$

when we set

$$\tilde{\phi}(f(X) + m_\alpha(X)) = \phi(f(X))$$

We now, by the same constuct as above arrive at isomorphisms:

$$\tilde{\phi_1} : \mathbf{K}_1[X]/ < f_1(X) > \rightarrow \mathbf{K}_1(\beta_1)$$

$$\tilde{\phi_2} : \mathbf{K}_2[X]/ < f_2(X) > \rightarrow \mathbf{K}_2(\beta_2)$$

But we know $\mathbf{K}_1(\beta_1) = \mathbf{L}_1$ and $\mathbf{K}_2(\beta_2) = \mathbf{L}_2$. Finally, the unique isomorphism $\sigma : \mathbf{L}_1 \rightarrow \mathbf{L}_2$ is

$$\sigma = \tilde{\phi_2}\sigma_0\tilde{\phi_1}^{-1}$$

. □

Lemma 3.4. *Let $\sigma_0 : \boldsymbol{K}_1 \rightarrow \boldsymbol{K}_2$ be an isomorphism of fields. Let $f_1(X) \in \boldsymbol{K}_1[X]$ and let $f_2(X) = \sigma_0(f_1(X)) \in \boldsymbol{K}_1[X]$. Let $\boldsymbol{L}_1$ be a splitting field of $f_1(X)$ and let $\boldsymbol{L}_2$ be a splitting field of $f_2(X)$. Then σ_0 extends to an isomorphism $\sigma : \boldsymbol{L}_1 \rightarrow \boldsymbol{L}_2$.*

Proof. Lets take the polynomial $f_1(X)$ and factor it into irreducible polynomials in $\mathbf{K}_1[X]$ (note: due to the isomorphism σ_0, we can use a notation $\mathbf{K}[X]$ both for $\mathbf{K}_1[X]$ and $\mathbf{K}_2[X]$). Lets denote the number of those factors by d. Obviously, d may vary from 1 to $deg(f_1(X))$. We define $n := deg(f_1(X)) - d$. To prove the statement of the lemma, we will do induction on n.

Base of induction: if $n = 0$, this means that already $f_1(X)$ can be written as a product of linear factors. This means that its splitting field is the same as the original field, by the definition of the splitting field, i.e. $\mathbf{L}_1 = \mathbf{K}_1(= \mathbf{K})$. The polynomial $f_2(X)$ is defined as $\sigma_0(f_1(X))$, and because σ_0 is an isomorphism, we know that $f_2(X)$ can then also be written as a product of linear factors, so by the same argument as before we see that $\mathbf{L}_2 = \mathbf{K}_2(= \mathbf{K})$, and from that it follows that $\sigma = \sigma_0$.
Suppose that our claim is true for all n up to some n_0, and let now $n > n_0$.

Clearly, $n > n_0$ implies that $n > 0$. This means that there exists a polynomial $g_1(X)$ such that it is an irreducible factor in $f_1(X)$ and that $deg(g_1(X)) \geq 1$. As $\mathbf{L}_1$ and $\mathbf{L}_2$ are splitting fields for $\mathbf{K}_1$ and $\mathbf{K}_2$ respectively, we can find an element $\alpha_1 \in \mathbf{L}_1$ such that $g_1(\alpha_1) = 0$ and $\alpha_2 \in \mathbf{L}_2$ such that $\sigma_0(g_1(\alpha_1)) = 0$. It is clear that $\mathbf{K}(\alpha_1) \subseteq \mathbf{L}_1$ and $\mathbf{K}(\alpha_2) \subseteq \mathbf{L}_2$.

We can now use the lemma 3.3 to obtain an isomorphism

$$\tilde{\sigma_0} : \mathbf{K}(\alpha_1) \rightarrow \mathbf{K}(\alpha_2)$$

such that $\tilde{\sigma_0} \mid_{\mathbf{K}} = \sigma_0$ and $\tilde{\sigma_0}(\alpha_1) = \alpha_2$.

Lets now define a new field $\mathbf{B} := \mathbf{K}(\alpha_1)$. We can look at the polynomial $f_1(X)$ now as a polynomial in $\mathbf{B}[X]$. We know that $\mathbf{L}_1$ is a splitting field of $f_1(X) \in \mathbf{B}[X]$, because it was a splitting field for $f_1(X) \in \mathbf{K}[X]$ and $\mathbf{B} \subseteq \mathbf{L}_1$ (and similarly for $\mathbf{L}_2$).

Since α_1 is an element of $\mathbf{B}$, we can see that when we factor $f_1(X)$ in $\mathbf{B}[X]$, it will have $(X - \alpha_1)$ as one of the irreducible factors, so it means that it will have at least one more irreducible factor in its factorisation than it had when we were in $\mathbf{K}[X]$. In turn, this means that that ($degree(f_1)-$the number of factors in its factorisation) is now smaller or equal n_0. So, we now use the induction hypothesis and obtain that σ_0 extends to an isomorphism σ.

□

Proposition 3.5. *Let $\boldsymbol{L}$ be a finite Galois extension of $\boldsymbol{K}$, so $\boldsymbol{L}$ is the splitting field of a separable polynomial $f(X) \in \boldsymbol{K}[X]$. Then $G = Gal(\boldsymbol{L}/\boldsymbol{K})$ is isomorphic to a permutation group on the roots of $f(X)$. If $f(X)$ is irreducible, then G is isomorphic to a transitive permutation group on the roots of $f(X)$.*

Proof. Consider the roots of the polynomial $f(X)$ and let us denote them by $\alpha_1,\ ...,\ \alpha_k$. The $\alpha_i \in \mathbf{L}$ because $\mathbf{L}$ is its splitting field of the polynomial $f(X)$. Let $\sigma \in \text{Gal}\ (\mathbf{L}/\mathbf{K})$. Because $\sigma \mid_{\mathbf{K}} = id$, it follows that $\sigma(f(X)) = f(X)$. Furthermore, $\sigma(\alpha_i)$ is the root of $\sigma(f(X)) = f(X)$, so we know that Gal $(\mathbf{L}/\mathbf{K})$ permutes the set of roots $\{\alpha_1,\ ...,\ \alpha_k\}$.

Suppose that $f(X) \in \mathbf{K}[X]$ splits in some extension $\mathbf{K} \subseteq \mathbf{B}$, and let us now consider $\alpha_1,\ ...,\ \alpha_k$ be the roots of $f(X) \in \mathbf{B}$, so that we can write $f(X) = (X - \alpha_1)^{d_1} \cdots (X - \alpha_k)^{d_k} \in \mathbf{B}[X]$. Then $\mathbf{J} := \mathbf{K}(\alpha_1,\ ...,\ \alpha_k)$ is a splitting field for $f(X)$ because it is clear that $f(X)$ splits over $\mathbf{J}$, and if we consider any other field over which $f(X)$ splits it must contain $\alpha_1,\ ...,\ \alpha_k$, hence it must contain $\mathbf{J}$, which makes $\mathbf{J}$ the smallest one with that property.

That why we can now conclude that $\mathbf{L} = \mathbf{K}(\alpha_1,\ ...,\ \alpha_k)$.
If $\sigma(\alpha_i) = \alpha_i\ , \forall i \Rightarrow \sigma = id$. This is the case if $\alpha_1,\ ...,\ \alpha_k$ are also elements of $\mathbf{K}$, and we have a trivial permutation group. We will clearly have some other permutations if there exists some i such that $\sigma(\alpha_i) \neq \alpha_i$.

If we are in the situation that $f(X)$ is irreducible, then none of the roots are in $\mathbf{K}$. Take now any two roots α_i and α_j. Using the lemma 3.3, we know that we can find an isomophism $\sigma_0 : \mathbf{K}(\alpha_i) \to \mathbf{K}(\alpha_j)$ such that $\sigma \mid \mathbf{K} = id$

and $\sigma_0(\alpha_i) = \alpha_j$. If we, then, use the lemma 3.4, we get that we can extend the isomorphism σ_0 to $\sigma : \mathbf{L} \to \mathbf{L}$. Because we have taken any two roots, we can clearly do the same proces for all of the roots, so we conclude that for any two elements $\alpha_i, \alpha_j \in A$ there exists $\sigma \in \Sigma$ such that $\sigma(\alpha_i) = \alpha_j$, i.e. the Galois group is isomorphic to the transitive permutation group.

□

3.2 Symmetric Functions

We would like to develop some theory on symmetric functions and symmetric group as it will assist us in finding the cycle lenghts in Galois group. Take an arbitrary field $\mathbf{A}$ and define $\mathbf{L} := \mathbf{A}(X_1, X_2, ..., X_n)$ to be the field of rational funcions. We now consider the symmetric group, which we may denote by S_n, acting on $\mathbf{L}$, i.e. permutations on the set $\{X_1, X_2, ..., X_n\}$.

Definition 3.6. The subfield $\mathbf{K} \subseteq \mathbf{L}$ that is fixed under S_n is called *field of symmetric functions* in $X_1, X_2, ..., X_n$. An element of $\mathbf{K}$ is called a *symmetric function.*

As $\mathbf{K} = \mathrm{Fix}(S_n)$, by definition we have that $\mathbf{L}$ is a Galois extension of $\mathbf{K}$.

Definition 3.7. The *elementary symmetric polynomials* $s_1, s_2, ..., s_n$ are:

$$s_k = \sum_{1 \le i_1 < i_2 < ... < i_k \le n} X_{i_1} \cdot X_{i_2} \cdots X_{i_k}, \ k = 1, ..., n$$

For example, if we take $n = 3$, we get $s_1 = X_1 + X_2 + X_3$, $s_2 = X_1 \cdot X_2 + X_1 \cdot X_3 + X_2 \cdot X_3$ and $s_3 = X_1 \cdot X_2 \cdot X_3$.

Lemma 3.8. *The field of symmetric functions* $\boldsymbol{K}$ *is* $\boldsymbol{A}(s_1, s_2, ..., s_n)$.

Lemma 3.9. *Let* $f(X_1, X_2, ..., X_n) \in \boldsymbol{L}$ *be a symmetric polynomial.Then we can uniquely write* $f(X_1, X_2, ..., X_n)$ *as a polynomial* $h(s_1, s_2, ..., s_n)$*, where* s_i *are elementary symmetric functions.*

3.3 Cycle lenghts in Galois group

Let us take look at separable polynomial $f(X) \in \mathbf{K}$. Denote the splitting field of this polynomial as $\mathbf{L}$ and denote the roots by $\{\alpha_1, \alpha_2, ..., \alpha_n\}$. Clearly, as $\mathbf{L}$ is the splitting field, $\alpha_i \in \mathbf{L}$, $\forall i$.

Denote by $G := \mathrm{Gal}(\mathbf{L}/\mathbf{K})$, by definition G, permutes $\{\alpha_1, \alpha_2, ..., \alpha_n\}$.

Let $\{Y_1, Y_2, ..., Y_n\}$ be a set of variables, and S_n be the symmetric group on the set $\{Y_1, Y_2, ..., Y_n\}$. By constructing an isomorphism $\phi : G \to G' \subseteq S_n$, $\phi(\sigma) = \sigma'$ such that $\sigma'(Y_i) = Y_j$ if $\sigma(\alpha_i) = \alpha_j$, we obtain G'.

We now introduce notation : $\tilde{\mathbf{K}} := \mathbf{K}[Y_1, Y_2, ..., Y_n]$, $\tilde{\mathbf{L}} := \mathbf{L}[Y_1, Y_2, ..., Y_n]$.

Define:

$$\theta := \alpha_1 \cdot Y_1 + \alpha_2 \cdot Y_2 + ... + \alpha_n \cdot Y_n \in \tilde{\mathbf{L}}$$

and:

$$F(Z) = \prod_{\sigma' \in S_n} (Z - \sigma'(\theta)) \in \tilde{\mathbf{L}}[Z] \qquad (*)$$

Note that $\sigma' \in S_n$ acts on the variables Y_i while it leaves the set α_i unchanged. $F(Z)$ is a polynomial in the variable Z, whose coefficients are polynomials in $\mathbf{L}[Y_1, Y_2, ..., Y_n]$. $F(Z)$ is also a symmetric function of its roots, which means we can now apply lemma 3.9 and from that it follows that we can write the coefficients of $F(Z)$ as polynomials of elementary symmetric functions of its roots.
To see what this means exactly, take a look at the following:

Lemma 3.10. *Consider the variables $X_1, X_2, ..., X_n$ over a field $\boldsymbol{K}$. If we take another variable, say X, we have:*

$$(X-X_1)(X-X_2)\cdots(X-X_n) = X^n - s_1X^{n-1} + \cdots + (-1)^i s_i X^{n-i} + \cdots + (-1)^n s_n$$

The idea of the proof is to multiply the left-hand side and to compute the coefficients for each power of X.

Now lets use the lemma above to determine some interesting facts. Lets consider a polynomial $f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$, with coefficients in $\mathbf{K}$. Let the roots of $f(X)$ be $\{\alpha_1, \alpha_2, ..., \alpha_n\} \in \mathbf{L} \supseteq \mathbf{K}$. What this means is that we can write

$$X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

Because evaluation of maps is a ring homomorphism, we wan evaluate the expression in lemma 3.10 at points $X_1 = \alpha_1, X_2 = \alpha_2, ..., X_n = \alpha_n$. From that we obtain that:

$$(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n) = X^n - s_1(\alpha_1, \alpha_2, ..., \alpha_n)X^{n-1} + \cdots$$

$$+(-1)^{n-1}s_{n-1}(\alpha_1, \alpha_2, ..., \alpha_n)X^{n-1} + (-1)^n s_n(\alpha_1, \alpha_2, ..., \alpha_n)$$

When we compare the two expressions for $(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$, we see that the coefficients of the $f(X)$ can be expressed in terms of its roots in the following way, for $i = 1, 2, ..., n$:

$$a_i = (-1)^i s_i(\alpha_1, \alpha_2, ..., \alpha_n)$$

From the above, we conclude that we can write the coefficients of $F(Z)$ as polynomials of variables $\{Y_1, Y_2, ..., Y_n\}$ and the coefficients of $f(X)$.

Hence, the coefficients of $F(Z)$ are polynomials in $\mathbf{K}[Y_1, Y_2, ..., Y_n]$, which we decided to denote by $\tilde{\mathbf{K}}$, i.e. $F(Z) \in \tilde{\mathbf{K}}[Z]$

We can now write $F(Z)$ as a product of irreducible factors in $\tilde{\mathbf{K}}[Z]$ as follows:

$$F(Z) = F_1(Z) \cdot F_2(Z) \cdots F_r(Z) \qquad (**)$$

As the identity is an element of S_n, we have that $(Z-\theta)$ is one of the factors in $(*)$, $(Z-\theta)$ divides a factor in $(**)$, when viewed in $\tilde{\mathbf{L}}[Z]$. We can rearrange the indices on the factors as we wish, so we assume, without the loss of generality, that $(Z-\theta)$ divides F_1. If we observe the form of $F(Z)$, we can consider the permutations on its factors by denoting $\tau'(Z-\theta) := (Z-\tau'(\theta))$. For a symmetric group S_n defined this way, by definition that $F(Z)$ is invariant under its actions, which means that the permutations in S_n permute the factors F_i, i.e. there is a permutation that sends F_1 to itself, another that sends it into F_2, F_3 ,...., F_k, and the same is true for other factors F_i.

Will we use the notation $(\star)$, to indicate the setup done above.

Lemma 3.11. *Let us be in $(\star)$, let $H' \subseteq S_n$ be the subgroup leaving $F_1(Z)$ invariant. Then $G' = H'$, and hence G is isomorphic to H'.*

Proof. Let us first write out: $H' = \{\tau' \in S_n \mid \tau'(F_1(Z)) = F_1(Z)\}$.

Because one of the linear factors in $F_1(Z)$ is $(Z-\theta)$, one of the linear factors in $\tau'(F_1(Z))$ is $\tau'(Z-\theta)$, which is the same as $Z-\tau'(\theta)$. So, we can conclude that $\forall \tau' \in S_n, \tau'(Z-\theta)$ divided $\tau'(F_1(Z))$.

Hence we can rewrite H' as follows $H' = \{\tau' \in S_n \mid \tau'(F_1(Z))$ divides $F_1(Z)\}$.

Furthermore, let us consider the composition of the permutations $\sigma \circ \sigma'$ acting on $\tilde{\mathbf{L}}$ (all $c := \sigma \circ \sigma' \in G \times G' \subseteq G \times S_n$). The isomorphism $\phi : G \to G' \subseteq S_n$, $\phi(\sigma) = \sigma'$ is defined such that $\sigma'(Y_i) = Y_j$ if $\sigma(\alpha_i) = \alpha_j$

which implies $\sigma \circ \sigma'(\theta) = \theta$, as we first do a permutation on Y_i and then apply the same permutation on α_i, effectively we have just changed the ordering of the summands in $\theta := \alpha_1 \cdot Y_1 + \alpha_2 \cdot Y_2 + ... + \alpha_n \cdot Y_n$.

$$\sigma \circ \sigma'(\theta) = \theta \Rightarrow \sigma(\theta) = \sigma'^{-1}(\theta)$$

Define:

$$G_1(Z) := \prod_{\sigma \in G} (Z - \sigma(\theta))$$

Considering how we have defined G_1 (we go through $\forall \sigma \in G$ to obtain the factors) it is clear that $\forall \sigma \in G$, $\sigma(G_1(Z)) = G_1(Z)$, i.e. $G_1(Z)$ is invariant under G. As defined, when the group of permutations in G is acting on $\mathbf{L}$, it leaves the set $\mathbf{K}$ invariant. Hence, when G acts on $\tilde{\mathbf{L}}$ it leaves $\tilde{\mathbf{K}}$ invarient. Since we have seen that $G_1(Z)$ is invariant under G, we conclude that $G_1(Z) \in \tilde{\mathbf{K}}[Z]$.

As the set of roots $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ does not have repeated elements, it means that the set $\{\sigma(\theta) \mid \sigma \in G\}$ has distinct elements as well. Applying the lemma 2.20, we get that $G_1(Z)$ is an irreducible as a polynomial in $\tilde{\mathbf{K}}[Z]$. Furthermore, one of the permutations in G is the identity permutation so we know that $(Z - \theta)$ occurs as a factor in $G_1(Z)$, and since both $G_1(Z)$ and $F_1(Z)$ are irreducible polynomials we must have that $G_1(Z) = F_1(Z)$. Also, $\tilde{\mathbf{L}} = \tilde{\mathbf{K}}(\theta)$. From all this we can deduce that the action S_n of the polynomials from $\tilde{\mathbf{L}}$ is determined by the action of S_n on θ.

Now, take an arbitrary $\tau' \in G'$. This implies that $G_1(Z) = F_1(Z)$ has $\tau'(Z - \theta)$ as one of the linear factors. This in turn, because of the definition of $G_1(Z)$, means that there exists $\sigma \in G$ such that $\tau'(Z - \theta) = Z - \sigma(\theta)$. We know that $\tau'(Z - \theta) = Z - \tau'(\theta)$, and also $Z - \tau'(\theta) = Z - (\sigma')^{-1}(\theta)$. When these three equalities are combined, we obtain:

$$Z - \tau'(\theta) = Z - (\sigma')^{-1}(\theta) \Rightarrow \tau' = (\sigma')^{-1} \Rightarrow \tau' \in G'$$

The last implication follows when we remeber that $\sigma \in G'$, and in addition that G' is closed with respect to inverse.

Conversely, if $\tau' \notin G'$, that means that $\tau'(Z - \theta) = Z - \tau'(\theta)$ is not a factor of $G_1(Z) = F_1(Z)$, so there does not exist a $\sigma \in G$ such that $\tau'(Z - \theta) = Z - \sigma(\theta)$. But then $\tau' \neq (\sigma')^{-1}$, in other words, $\tau' \notin G'$, which concludes our proof.

□

Definition 3.12. Let $f(X) \in \mathbf{K}[X]$ be a polynomial of degree n with roots $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ in some field $\mathbf{L}$ in which $f(X)$ splits. Let:

$$\delta = \prod_{i<j}(\alpha_i - \alpha_j)$$

and define:

$$\Delta := \Delta(f(X)) = \delta^2$$

Theorem 3.13. *Let $f(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n and let p be a prime not dividing the discriminant of $f(X)$. Let furthermore $\bar{f}(X) = \prod_{i=1}^{r} \bar{f}_i(X)$ be the factorisation into irreducible polynomials in the ring $\mathbb{F}_p[X]$, where $\overline{f}(X)$ is the reduction of $f(X)$ modulo p. Then the Galois group of $f(X)$, seen as a subgroup of S_n, containst an element whose cycle lengths are precisely the degrees of the $\bar{f}_i$.*

Proof.
Denote the roots by $f \in \mathbb{Z}[X]$ by $\{\alpha_1, \alpha_2, ..., \alpha_n\}$.
Since $f(X)$ is an irreducible polynomial $\Rightarrow \alpha_i \neq \alpha_j,\ \forall i \neq j \Rightarrow \Delta(f(X)) \neq 0$.
If $p \mid \Delta(f(X)) \Rightarrow p \mid (\alpha_i - \alpha_j) \Rightarrow \alpha_i \equiv \alpha_j\ mod(p)$. So the condition that p does not divide the discriminant ensures that the irreducible factors $\overline{f_i}$ all have distinct roots.

From $f(X)$, we will repeat the construction $(\star)$, to obtain a a polynomial $F(Z)$. From the lemma 3.9, we can (as before) see that because $F(Z)$ is a symmetric functions of its roots, its coefficients are actually polynomials in the coefficients of $f(X)$, and if we combine this with the the fact that a monic polynomial in $\mathbb{Z}[X]$ is irreducible if and only if it is irreducible as a polynomial in $\mathbb{Q}[X]$, to see that the factorisation of the polynomial $F(Z)$ in $\mathbb{Q}[Y_1, Y_2, ..., Y_n]$ can be seen as a factorisation in $\mathbb{Z}[Y_1, Y_2, ..., Y_n]$. We have:

$$F(Z) = F_1(Z) \cdot F_2(Z) \cdots F_r(Z)$$

where $F_i(Z)$ is now an irreducible elemet in $\mathbb{Z}[Y_1, Y_2, ..., Y_n][Z]$,
$\forall i = \{1, 2, ..., r\}$.

We now do the reduction modulo p on each of the $F_i(Z)$ and we obtain:

$$\bar{F}(Z) = \bar{F}_1(Z) \cdot \bar{F}_2(Z) \cdots \bar{F}_r(Z)$$

where $\bar{F}_i(Z)$ is now an elemet $\mathbb{F}_p[Y_1, Y_2, ..., Y_n][Z], \forall i = \{1, 2, ..., r\}$. We do not know if $\bar{F}_i(Z)$ is still irreducible.

If $\bar{F}_i(Z)$ are not irreducible, it means that they can be written as a product of irreducible factors so let us, for $\forall i = \{1, 2, ..., r\}$ and $\forall j$, denote the set of irreducible factors of $\bar{F}_i(Z)$ by $\{\bar{F}_{i,j}(Z)\}$. So $\bar{F}_{1,1}(Z)$ is an irreducible factor in $\bar{F}_1(Z)$. We do not care about the index j, other that we use it to be able to take into consideration a particular irreducible factor of $\bar{F}_i(Z)$.

Lets take the symmetric group S_n acting on $\mathbb{F}_p[X_1, X_2, ..., X_n]$, and define $\bar{K}' := \{\tau' \in S_n \mid \tau'(\bar{F}_{1,1}(Z)) = \bar{F}_{1,1}(Z)\}$. From lemma 3.11, it follows that $\bar{K}'$ is isomorphic to $\mathrm{Gal}(\bar{\mathbf{L}}/\mathbb{F}_p)$, where $\bar{\mathbf{L}}$ is the splitting field of $\bar{f}(X)$ over $\mathbb{F}_p$.

On the other hand, since the roots of $\bar{f}_i$ are distinct it means that all permutations that fix an irreducible factor in $\bar{F}_i(Z)$ are also distinct, and from this we can proceed and say that each $\bar{F}_i(Z)$ has distinct roots, and $i \neq j \Rightarrow \bar{F}_i(Z)$ and $\bar{F}_j(Z)$ have no common roots. In particular, this means that if a permutation preserves one irreducible factor of $\bar{F}_i(Z)$, it has to preserve all irreducible factors of $\bar{F}_i(Z)$, i.e. the whole $\bar{F}_i(Z)$. In our situation it means that each permutation that preserves $\bar{F}_{1,1}(Z)$, preserves $\bar{F}_1(Z)$. So,

$$\bar{K}' = \{\tau' \in S_n \mid \tau'(\bar{F}_{1,1}(Z)) = \bar{F}_{1,1}(Z)\} \subseteq \{\tau' \in S_n \mid \tau'(\bar{F}_1(Z)) = \bar{F}_1(Z)\}$$

However, $\{\tau' \in S_n \mid \tau'(\bar{F}_1(Z)) = \bar{F}_1(Z)\}$, i.e. the set that was denoted by H' in the previous lemma is the Galois group of the polynomial $f(X)$ in the notation $G :=\mathrm{Gal}(\mathbf{L}/\mathbb{Q})$, where $\mathbf{L}$ is the splitting field of $f(X)$ over $\mathbb{Q}$.

Take a look at $\bar{K}' = \{\tau' \in S_n \mid \tau'(\bar{F}_{1,1}(Z)) = \bar{F}_{1,1}(Z)\}$ further. $\bar{K}'$ is cyclic, i.e. generated by a single element, as it is a subgroup a Galois group, which is always cyclic. This means that $\bar{K}'$ can be generated by powers of a single permutation. We can hence write this one permutation as a product of cycles: $(1\ 2\ 3\ ...\ j) \cdot (j+1\ ...) \cdot \cdot\cdot$, with each of those cycles transitive on the roots of $\bar{F}_{1,1}(Z)$.

From the proposition 3.5, we know that each transitive set corresponds to one irreducible factor of $\bar{f}(X)$, which we have denoted $\bar{f}_i(X)$. Let us first adjust the indices i on $\bar{f}_i(X)$ if necessary, such that $\bar{f}_i(X)$ corresponds to the $i-th$ cycle. We extend our notion of this correspondence from the $i-th$ cycle to elements in the $i-th$ cycle and also from $\bar{f}_i(X)$ to the roots of $\bar{f}_i(X)$, and so we see that each root corresponds to one of the numbers in the same cycle. From that, and if we remeber that we only have distinct roots, we can see that the lenght of a $i-th$ cycle corresponds exacly to the degree of $\bar{f}_i(X)$, $\forall i$.

Because $\bar{K}' \subseteq G$ is a subgroup of G, it follows that G also has the permutation of the same type. □

4 Sufficient conditions for $G \cong S_n$

In this section we shall try to find theorems stating sufficient conditions for permutation groups to be the symmetric group. We know that the group S_n is generated by its cycles. The following theorems are mostly from [7]. First we note a useful lemma.

Lemma 4.1. *For a k-cycle* $(i_1\ i_2\ ...\ i_k)$ *in* S_n *and any* $\sigma \in S_n$,

$$\sigma(i_1\ i_2\ ...\ i_k)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ ...\ \sigma(i_k)).$$

4.1 Criterion used in our Sage computations

Here we would like to present the criterion that we will be using in our Sage computations as it provides easy-to-check conditions concerning only the cycle lenght.

Theorem 4.2. *Let* G *be a transitive subgroup of* S_n. *Suppose* G *contains a* $2-$*cycle and an* $(n-1)-$*cycle. Then* $G \cong S_n$.

Proof. Let r be the $(n-1)-$*cycle*. We can do the relabeling if it is necessary and from now on assume that $r = (1\ 2\ ...n-1)$. Then, our transposition is $t = (i\ j)$, for some $i, j \in \{1, 2, ..., n\}$ (possibly different than in the beginning). Lets denote by G our transitive permutation group. Because G is transitive on the set $\{1, 2, ..., n\}$, we know that there exists $\sigma \in G$ such that $\sigma(j) = n$. This in turn means that $\sigma(i) = k$, for some k. By applying the lemma 4.1 we get:

$$\sigma(i\ j)\sigma^{-1} = \sigma(i)\sigma(j) = (k\ n) =: t_k$$

Let us show that we can get all the permutations of the type $(i\ n)\ \forall i$. Consider the following: $r^i t_k r^{-i}$. By similar direct calculation it follows that $r^i t_k r^{-i} = ((k+i)\ n)$.. Lets denote it in consistency to above notations as $((k+i)\ n) =: t_{k+1}$ Keep in mind that $k+i$ is actually taken modulo $n-1$, which only makes sense.
Finally we can look at the following: $t_i\ t_j\ t_i^{-1} = (i\ n)(j\ n)(i\ n)^{-1}$. Quick calculation shows that $t_i\ t_j\ t_i^{-1} = (i\ j),\ \forall i \neq j$.
By this we have showed that G contains all transpositions. The theorem 4.3 shows that S_n is generated by its transpositions. Therefore, $G = S_n$.
□

4.2 General case

Theorem 4.3. *For $n \geq 2$, S_n is generated by its transpositions.*

Proof. This is clear for $n = 1$ and $n = 2$. For $n \geq 3$, we note $(1) = (1\ 2)^2$ and every cycle of length > 2 is a product of transpositions:

$$(i_1\ i_2\ ...\ i_k) = (i_1\ i_2)(i_2\ i_3)...(i_{k-1}\ i_k)$$

Since the cycles generate S_n, and the product of transpositions gives us all cycles, the transpositions generate S_n.

□

Theorem 4.4. *For $n \geq 2$, S_n is generated by $n-1$ transpositions*

$$(1\ 2),\ (1\ 3),\ ...,\ (1\ n).$$

Proof. The theorem is obvious for $n = 2$, so we take $n \geq 3$. By theorem 4.3, it suffices to write any transposition in S_n as a product of the transpositions involving element 1. But for a transposition $(i\ j)$ it is clear that:

$$(i\ j) = (1\ i)(1\ j)(1\ i)$$

□

Theorem 4.5. *For $n \geq 2$, S_n is generated by $n-1$ transpositions*

$$(1\ 2),\ (2\ 3),\ ...,\ (n-1\ n).$$

Proof. By theorem 4.3, it suffices to show any transposition $(a\ b)$ in S_n in a product of transpositions of the form $(i\ i+1)$ where $i < n$. Since $(a\ b) = (b\ a)$, we can assume without a loss of generality that $a < b$. We will argue by induction on $b - a$ that $(a\ b)$ is a product of traspositions $(i\ i+1)$. This is obvious when $b - a = 1$, since $(a\ a+1)$ is one of the transpositions we want in the desired generating set. Now suppose that $b - a = k > 1$ and the theorem is settled for all transpostitions moving a pair of integers whose difference is less than k. Consider the formula:

$$(a\ b) = (a\ a+1)(a+1\ b)(a\ a+1)$$

The first and the third transposition on the right side lie in our desired generating set. The middle transposition permutes a pair of integers with difference $b - (a+1) = k - 1 < k$. By the induction hypothesis, $(a+1\ b)$ is a product of transpositions $(i\ i+1)$, so $(a\ b)$ is as well.

□

Theorem 4.6. *For $n \geq 2$, S_n is generated by the transposition $(1\ 2)$ and the n-cycle $(1\ 2\ ...\ n)$.*

Proof. By theorem 4.5, it suffices to show products of permutations $(1\ 2)$ and $(1\ 2\ ...\ n)$ yield all transpositions of the form $(i\ i+1)$. We may take $n \geq 3$. Set $\sigma = (1\ 2\ ...\ n)$. Then

$$\sigma(1\ 2)\sigma^{-1} = (\sigma(1)\ \sigma(2)) = (2\ 3)$$

and more generally for $k = 1,\ 2,\ ,...,\ n-2$,

$$\sigma^k(1\ 2)\sigma^{-k} = (\sigma^k(1)\ \sigma^k(2)) = (k+1\ k+2)$$

□

4.3 Condition applicable to Galois theory

From what we have just seen, it seems that there are plenty theorems that provide sufficient conditions for permutation groups to be the symmetric group. However, none of them are applicable to our case, for we have a method of determining the Galois group that can only provide the cycle lenght of the permutation and not the exact elements that make that cycle. While if we have $n-1$-cycle and a transposition, we can always do the relabeling of the roots to get again a transposition and $n-1$-cycle that is of the form $(1\ 2\ ...\ n-1)$, we cannot do such relabeling to recreate the conditions of these other theorems. However, we have one more theorem to present that has some, although limited, application in what we are trying to achieve.

In particular, we can use it if $n = p$, where p is a prime number. Since $1 \leq a < b \leq p$, we know that the difference $(b-a) \in \{1, 2, ..., p-1\} \Rightarrow gcd(b-a, p) = 1$. In that case, we understand it as: any transposition and a p-cycle generate S_p.

Theorem 4.7. *For $1 \leq a < b \leq n$, transposition $(a\ b)$ and n-cycle $(1\ 2\ ...\ n)$ generate S_n if and only if $gcd(b-a, n) = 1$.*

Proof. Let $d := gcd(b-a, n)$. We show that every $g \in <(a\ b),\ (1\ 2\ ...\ n)>$ preserves mod d congruences among $\{1,\ 2,\ ...\ , n\}$.

$$i \equiv j\ mod\ (d) \Rightarrow g(i) \equiv g(j)\ mod\ (d) \qquad (*)$$

It suffices to check this when $g = (a\ b)$ and when $g = (1\ 2\ ...\ n)$. For i different form a and b, $(a\ b)(i) = i$. Also, $(a\ b)(a) = b \equiv a\ mod\ (d)$ and

$(a\ b)(b) = a \equiv b\ mod\ (d)$, so $(a\ b)(i) \equiv i\ mod\ (d)$, for all i. Thus the above congruence $(*)$ holds or $g = (a\ b)$. As for $g = (1\ 2\ ...\ n)$, we have $(1\ 2\ ...\ n)(i) \equiv i\ mod\ (n)$, so also $(1\ 2\ ...\ n)(i) \equiv i\ mod\ (d)$, since $d \mid n$. Therefore,

$$i \equiv j\ mod\ d \Rightarrow i + 1 \equiv j + 1\ mod\ (d)$$

so $(*)$ holds for $g = (1\ 2\ ...\ n)$.

For $d > 1$, the group S_n does not preserve mod d congruences : pick $i \not\equiv j\ mod\ (d)$ and consider the transposition $(i\ j)$. So if $< (a\ b),\ (1\ 2\ ...\ n) >= S_n$, then we must have $d = 1$.

Conversely, let $gcd(b-a, n) = 1$. Let $\sigma = (1\ 2\ ...\ n)$, so $\sigma^i(a) \equiv a+i\ mod\ (n)$. Therefore $\sigma^{b-a}(a) \equiv b\ mod\ (n)$, and both sides of the congruence are between 1 and n, so $\sigma^{b-a}(a) = b$. Since $(b - a, n) = 1$, $< \sigma >=< \sigma^{b-a} >$ and σ^{b-a} is an n-cycle sending a to b, so $\sigma^{b-a} = (a\ b\ ...)$ (where dots are some other numbers in the range $\{1,\ 2,\ ...,\ n\}$). Then:

$$< (a\ b),\ \sigma > = < (a\ b),\ \sigma^{b-a} > =< (a\ b),\ (a\ b\ ...) >$$

A suitable relabelling of numbers $1,\ 2,\ ...,\ n$ turns $(a\ b)$ into $(1\ 2)$ and $(a\ b\ ...)$ into $(1\ 2\ ...\ n)$, so $< (a\ b),\ \sigma >$ is a conjugate to $< (1\ 2),\ (1\ 2\ ...\ n) >$, which is S_n by theorem 4.6.

□

5 Computations in Sage

We have created a program in Sage to test the Maeda's conjecture.

First, we generate a newform of level N and weight k. Then we extract a defining polynomial f of a number field of coefficients of a newform. We apply a function *is_symm* on the polynomial f in order to validate the conjecture.

We have defined a bool function *is_symm* that takes two arguments, an irreducible monic polynomial f with coefficients in $\mathbb{Z}$ and range (if undefined, we take range = 10000). For the prime numbers p within the range, we do the factorisation of polynomial f modulo p. Since we know that degrees of the factors correspond to cycle lenghts in the Galois group, we are checking the sufficient criterion (Theorem 4.2) for the subgroup of symmetric group to be the whole symmetric group. In other words, if $n = deg(f)$, we are trying to

find an irreducible factor of degree $n-1$ and an irreducible factor of degree 2 (but we then also require all the other degrees to be odd). If both conditions are satisfied, our function returns true.

On a 2.4Hz Mac computer from 2010 with a 4GB of RAM, we managed to compute results for levels $N = 2, 3, 5, 6$ and 7 and weight $k \leq 32$. Originally, we wanted to check squarefree levels up to 21. Our results experimentally verified the conjecture. Here the exact code used to do so.

```
R.<x>=PolynomialRing(ZZ,'x',implementation='NTL')

def is_symm(f,r=10000):
 c1=0
 c2=0
 p=0
 n=f.degree()
 for p in range(r):
  if is_prime(p):
   L=f.factor_mod(p)
   j=0
   count_odd=0
   while j<len(L):
    if (L[j][0]^L[j][1]).degree()==n-1:
     c1=1
     if (L[j][0]^L[j][1]).degree()==2:
     k=0
      while k<len(L):
       if gcd((L[k][0]^L[k][1]).degree(),2)==1:
        count_odd=count_odd+1
        k=k+1
       else:
        k=k+1
        continue
      if (count_odd==(len(L)-1)):
       c2=1
      count_odd=0
      j=j+1
    if (c1==1) and (c2==1):
     return true
    else: continue
```

```
   else: continue
  return false

L = [2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 35]
i=0
n=1
for i in range(14):
 n = n*L[i]
 k=2
 while k<40:
  N = Newforms(n,k,names='a')
  j=0
  while(j < len( N )):
   if(N[j].hecke_eigenvalue_field().degree()>2):
    f = (N[j].hecke_eigenvalue_field().defining_polynomial())
    is_symm(f)
    j = j + 1
    k=k+2
```

References

[1] D.J.H. Garling: *A course in Galois theory* 1986: Cambridge University Press

[2] Steven H. Weintraub: *Galois Theory - Second Edition* 2009: Springer

[3] B. L. van der Waerden: *Modern Algebra* 1949.

[4] Jean-Pierre Escofier: *Galois Theory* 2001: Springer

[5] Ian Stewart: *Galois Theory - Third Edition* 1945: Chapman & Hall/CRC

[6] Wolfram Alpha: *Symmetric Group* http://mathworld.wolfram.com/SymmetricGroup.html: last accessed: November, 2014.

[7] Keith Conrad: *Generating Sets* http://www.math.uconn.edu/ kconrad/blurbs/grouptheory/genset.pdf