COMPUTING GALOIS GROUPS

R. AGRAWAL, H. CHEN, J. FINKELSTEIN, M. STEPHENSON

1. Mathematical Preliminaries

This section covers concepts that will be used or alluded to in the rest of the document.

Definition 1. Polynomials are soluble by radicals if roots can be expressed in terms of addition, subtraction, multiplication, division, and the extraction of roots.

Tha Galois groups of a polynomial f of degree n is isomorphic to a subgroup of S_n. Hence, Gal(f) permutes the roots of $f(x) = 0$. Renumbering the roots of Gal(f) brings us to a conjugate subgroup of S_n, so we bring our attention to the conjugacy class of subgroups.

Definition 2. In a group G, elements a, b are conjugate if there exists an element $g \in G$ such that $a = g^{-1}bg$. We say that a, b are in the same conjugacy class. In an Abelian group, each conjugacy class can have only one element.

Definition 3. Let G be a permutation group on $\{1, 2, 3, \ldots n\}$, then G is transitive if for all $i, \leq n$ there exists γ such that $\gamma(i) = j$. Equivalently, it is enough to show that for all $i \leq n$ there exists λ such that $(1) = i$.

The above definitions give us the machinery to explore solubility using a Galois group.

Theorem 1.1. *Let L be a splitting field of a separable polynomial $f \in F[x]$ of degree n. The the subgroup of S_n corresponding to Gal(L/F) is transitive if and only if f is irreducible over F, equivalently the Galois group Gal(f) is transitive over the set of zeroes of f.*

Proof. Sketch: (1) Suppose that f is irreducible and has roots $1, a_2 \ldots, a_n \in L$. Construct an automorphism $\sigma : L \equiv L$ that takes a_i to a_j. The corresponding permutation in S_n to $\sigma \in$ Gal(f) takes i to j and is the identity on F, thus Gal(f) is transitive.
(2) Suppose that Gal(f) corresponds to a transitive subgroup of S_n, and let h be an irreducible factor of f. Showing that $deg(h) \geq n$ implies that f is irreducible. Let the roots of $f = a_1, a_2, \ldots, a_n$. Since h is a non-constant factor from being irreducible, there must be a_i such that $h(a_i) = 0$. By transitivity, there exists $\gamma \in$ Gal(f) such that $\gamma(a_i) = a_j$.We know that h has coefficients in F, so $\gamma(a_i) = a_j$ is also a root of h. Since the choice of γ, a_j is arbitrary and iterable for all n, it follows that h has n roots, showing that f is irreducible.

□

Definition 4. The normal form of a polynomial of degree n is $x^n + ax + b$. All intermediate x^k for $n > k > 1$ have coefficients set to 0.

Tschirnhaus introduced transformations that were useful in solving cubics and quartics by rephrasing the polynomial in its normal form. His transformations failed to help with quintics by often making the problem of solving a quintic into solving a sextic. Galois theory provides that there are rational roots of the sextic resolvent if and only if the corresponding quintic is solvable by radicals.

Definition 5. Tschirnhaus transformation: Given a polynomial $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, defining $y = b_0 + b_1x + +\_n - 1x^{n-1}$ to obtain a rephrasing of the polynomial where $x^{n-1}, x^{n-2}, x^{n-3}$ terms have been eliminated, which in the quintics case gives us the normal form with $f = x^5 + px + q = 0$.

Excercise 6. Find a transformation so that $f = x^3 + a_1x^2 + a_2x + a_3 = 0$ can be rephrased with the term x^2 eliminated.

Excercise 7. Find a transformation so that $f = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0$ can be rephrased with the term x^4 eliminated.

2. Introduction and Motivation

The majority of this material relies on Cox [2].

Stewart points out that the big question motivating algebra is to find out how to solve a type of equation. Learning to compute Galois groups is an endeavor in this direction. Before we explore the machinery and results to pursue this, we paint a broad strokes picture of the complexity of taking on the computation.

The discussion assumes the universe of the generalized Riemann hypothesis. It hinges on the fact that finding the order of a Galois group is useful in finding the Galois group.

An interesting lens to hold might be that Galois' work can be though of as making Abel-Ruffini computable, thus providing a decision algorithm to finding solutions of polynomials. Admittedly, this algorithm has many components and has been worked upon by many mathematicians in the years after Galois to produce results as follows. Some of the intermediate work in making the algorithm usable is discussed in the remainder of the document.

Theorem 2.1. *The order of the Galois group G of a monic polynomial $f \in \mathbb{Z}[x]$ is computable in P^P.*

The algorithm first counts the number of split primes less that a suitably large x using a single P query. The order of the Galois group is the nearest integer to $\frac{1}{\pi_1(x)}\frac{x}{\ln(x)}$, where $\pi_1(x)$ is the conjugacy class. This can be computed in polynomial time.

Theorem 2.2. *Let f have nonzero degree n, let s be the size of the binary encoding of f. For any constant $c > 0$ there is a BPP^{NP} algorithm that computes an approximation A of $|G|$ such that*

$$(1 - \tfrac{1}{s^c})A \leq |G| \leq (1 + \tfrac{1}{s^c})A$$

with probability greater than $2/3$.

This result is useful in that for polynomials f, g with nonzero discriminant, such that the splitting field of $\mathbb{Q}_g$ of g is contained in the splitting field $\mathbb{Q}_f$ of f, and $[\mathbb{Q}_f : \mathbb{Q}_g]$ is of a prime power, there is a BPP^{NP} algorithm to compute the order of G, assuming G has already been computed (described computationally).

3. Quartics

The quartics do not require any of the new machinery that has not yet been described. It is well explored in the primary text.

Theorem 3.1. *Given a field F with characteristic $\neq 2$ and $f \in F[x]$ be a monic, irreducible quartic polynomial.*
Given that the characteristic of F does not divide deg(f) we have that f is separable and $f = x^4 - c_1x^3 + c_2x^2 - c_3x + c_4$ with $c_1, c_2, c_3, c_4 \in F$.
We have the discriminant $\Delta(f) = 144c_2c_1^2c_4^2 + 18c_1c_3^3c_2 - 192c_1c_3c_4^2 - 6c_1^2c_3^2c_4 + 144c_4c_3^2c_2 - 4c_2^3c_1^2c_4 + c_2^2c_1^2c_3^2 + 256c_4^3 - 27c_3^4 + 18c_1^3c_3c_2c_4 - 4c_1^3c_3^3 + 128c_2^2c_4^2 + 16c_2^4c_4 - 4c_2^3c_3^2 - 27cc_1^4c_4^2 - 80c_2c_1c_3c_2^2c_4$.
We have the ferrari resolvent $\theta_f(y) = y^3 - c_2y^2 + (c_1c_3 - 4c_4)y - c_3^2 - c_1^2c_4 + 4c_2c_4$.
Then the subgroup $G \in S_4$ is determined as follows:

- *If $\theta_f(y)$ is irreducible over F, then if $\Delta(f) \notin F^2, G = S_4$, otherwise $G = A_4$.*
- *If $\theta_f(y)$ splits completely over F, then $G = \langle((12)(34), (13)(24)\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*
- *If $\theta_f(y)$ has a unique root $\in F$ then G is conjugate to $\langle(1324), (12)\rangle \simeq D_8$ if $4+c_1^2-4c_2 \neq 0$ and $\Delta(f)(4+c_1^2-4c_2) \notin (F^*)^2$ or $4+c_1^2-4c_2 = 0$ and $\Delta(f)(^2-4c_4) \notin (F^*)^2$. Otherwise G is conjugate to $\langle(1324)\rangle \simeq \mathbb{Z}/\mathbb{Z}$.*

Proof. Proof intuition for item 1: For item 1, the evaluation map to the roots of f in its splitting field can be used to rephrase the Ferrari resolvent and find its roots in terms of the roots of f in the splitting field. Applying the tower theorem gives us $[L : F] = 12$, and the only subgroup of S_4 with 12 elements if A_4. Thus, the dichotomy of finding G holds.

The remainder of the proof is available in Cox, and involves tremendous case analysis. □

Excercise 8. Using the above, prove that $\text{Gal}(f) = S_4$ for $f = x^4 - x - 1 \in \mathbb{Q}[x]$.

4. Resolvent

Definition 9. Given a field F, and a rational function $f \in F(x_1, x_2, ..., x_n)$ we consider the the rational functions $\sigma \cdot f$ for all $\sigma \in S_n$. We will denote these distinct rational functions $f_1, ..., f_m$. We now look at the polynomial

$$\theta(x) = \prod_{i=1}^{m}(x - f_i);$$

that is, the polynomial with roots $f_1, ..., f_m$. This polynomial is called the *resolvent polynomial* of f.

Example 10. Consider the function $z_1 = \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3)$ where $\omega = e^{2\pi i/3}$. We note that S_3 acting on z_1 gives us $z_1, z_2 = (23) \cdot z_1, \omega z_1, \omega z_2, \omega^2 z_1$, and $\omega^2 z_2$. So, the resolvent of z_1 is:

$$\begin{aligned}\theta(z) &= (z - z_1)(z - z_2)(z - \omega z_1)(z - \omega z_2)(z - \omega^2 z_1)(z - \omega^2 z_2) \\ &= z^6 + qz^3 - \frac{p^3}{27}\end{aligned}$$

where

$$\begin{aligned}q &= -\frac{2\sigma_1^3}{27} + \frac{\sigma_1\sigma_2}{3} - \sigma_3 \text{ and} \\ p &= -\frac{\sigma_1^2}{3} + \sigma_2.\end{aligned}$$

Example 11. Consider $y_1 = x_1x_2 + x_3x_4 \in F(x_1, x_2, x_3, x_4)$. We know S_4 acting on y_1 gives us $y_1, y_2 = x_1x_3 + x_2x_4$, and $y_3 = x_1x_4 + x_2x_3$. So, the resolvent of y_1 is

$$\begin{aligned}\theta(y) &= (y - (x_1x_2 + x_3x_4))(y - (x_1x_3 + x_2x_4))(y - (x_1x_4 + x_2x_3)) \\ &= y^3 - \sigma_2 y^2 + (\sigma_1\sigma_3 - 4\sigma_4)y - \sigma_3^2 - \sigma_1^2\sigma_4 + 4\sigma_2\sigma_4.\end{aligned}$$

There are a few "universal" resolvents which are resolvent polynomials for all functions of degree n. These include the universal Ferrari resolvent/universal cubic resolvent (which is example 3 of this section) and a universal sextic resolvent that will be gone over in the section on quintic polynomials.

The understandable question to now ask is: why do we need/want the resolvent? How does it help us?

The main use of resolvent polynomials is in Jordan's Strategy, which is considered one of the best modern methods of computing Galois groups. Due to time constraints, we will only briefly go over Jordan's Strategy to see how resolvent polynomials are used and instead focus on Kronecker more in-depth.

4.1. **Jordan's Strategy.** Jordan's Strategy is broken into five steps for computing Galois groups. The first is **Classify Groups**.

This has already been done for all transitive subgroups $G \subseteq S_n$ for $n \leq 32$.
The second step is **Find polynomials**.

For every transitive subgroup $G \subseteq S_n$ classified from the previous step, find a polynomial φ in $x_1, ..., x_n$ with symmetry group $H(\varphi)$. Stauduhar lists such a polynomial for each transitive subgroup S_4, S_5, S_6^*, and S_7.
*: Errors were made in calculating these polynomials, they are noted in the textbook by Cox.
Next we **Compute resolvents**.

We take G and φ from step 2 and compute the resolvent in the universal case for φ. We write the resolvent's coefficients in terms of the elementary symmetric polynomials:

$$\begin{aligned} e_0(x_1, ..., x_n) &= 1 \\ e_1(x_1, ..., x_n) &= \sum_{1 \le i \le n} x_i \\ e_2(x_1, ..., x_n) &= \sum_{1 \le i < j \le n} x_i x_j \\ &... \\ e_n(x_1, ..., x_n) &= x_1 \cdot ... \cdot x_n. \end{aligned}$$

We then specialize to the coefficients of the polynomial f whose Galois group we are attempting to calculate. Assuming the roots of f are $\alpha_1, ..., \alpha_n$, this makes our resolvent

$$\Theta_f(y) = (y - \varphi_1(\alpha_1, ..., \alpha_n))...(y - \varphi_m(\alpha_1, ..., \alpha_n)).$$

Our next step is **Use resolvents**.

Assume $f \in F[x]$ is irreducible and separable of degree n and with φ (with symmetry group $H(\varphi) \subseteq S_n$) give the resolvent $\Theta_f(y) \in F[y]$. We then can find the Galois group G_f using the resolvent with Proposition 13.3.2 from the textbook, which is as follows:

Theorem 4.1. *Let $f \in F[x]$ be separable and irreducible of degree n.*

(1) If G_f is conjugate to a subgroup of $H(\varphi)$, then $\Theta_f(y)$ has a root in F.
(2) If $\Theta_f(y)$ has a simple root in F, then G_f is conjugate to a subgroup of $H(\varphi)$.

We can now move on to the final (not always necessary) step: **Repair resolvents**.

It might happen that the resolvent computed previously fail when their rational roots aren't simple. The way to solve this is via a method called a *Tschirnhaus transformation*, which we will not be able to go over.

4.2. **Exercises.**

Excercise 12. What is the resolvent polynomial of $g = x_1 + x_2 + x_3$ over $\mathbb{Q}$?

Excercise 13. What is the resolvent polynomial of $g = x_1 + \omega x_2 + x_3 x_4$ over $F(x_1, x_2, x_3, x_4)$?

4.3. **Bibliography.** Cox, D. A., Ebrary, I. (2012). *Galois theory.* John Wiley Sons.

5. Quintic

5.1. **Classification of transitive subgroups of S_5.**

Lemma 14. TFAE:

(1) G is transitive.
(2) $5||G|$.
(3) G contain a five cycle.

Proof. Left as an exercise. □

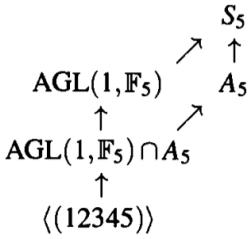
Definition 15. The one-dimension affine linear group $\mathrm{AGL}(1,\mathbb{F}_5)$ consists of maps $i \mapsto ai+b$, where $i,a,b \in \mathbb{F}_5$. If we regards $\{1,2,3,4,5\}$ as congruence classes modulo 5, then $\mathrm{AGL}(1,\mathbb{F}_5) \subset S_5$.

Lemma 16. Generators:

(1) $\mathrm{AGL}(1,\mathbb{F}_5)$ is generated by (12345) and (1243), so it has order 20.
(2) $\mathrm{AGL}(1,\mathbb{F}_5) \cap A_5$ is generated by (12345) and (14)(23).
(3) Up to conjugacy the transitive subgroups of $\mathrm{AGL}(1,\mathbb{F}_5)$ are $\mathrm{AGL}(1,\mathbb{F}_5)\cap A_5, \langle(1,2,3,4,5)\rangle$.

Proof. Left as an exercise. □

Theorem 5.1. *Every transitive subgroup $G \subset S_5$ is given by the following figure up to conjugacy.*



Proof. First suppose $\theta = (12345)$ and $\langle\theta\rangle$ is the only transitive subgroup (of order 5) in G, immediately it follows that $g\langle(12345)\rangle g^{-1} = \langle(12345)\rangle$ for all $g \in G$, implying G is contained in the normalizer of $\langle\theta\rangle$. Denote the normalizer $N_{S_5}(\langle\theta\rangle)$, and we prove that $N_{S_5}(\langle\theta\rangle) = \mathrm{AGL}(1,\mathbb{F}_5)$. Consider

$$\tau \in N_{S_5}(\langle\theta\rangle) \Leftrightarrow \tau\theta = \theta^l\tau \text{ for some } 1 \le l \le 4.$$

Because $\theta = (12345)$ is a translation, $\theta^l(i) = i + l$, so the following two identities are equivalent

$$\tau\theta = \theta^l\tau \Leftrightarrow \tau(i+1) = \tau(i) + l.$$

Iterate the procedure on the right hand side to see that for $j \in \mathbb{Z}_+$,

$$\tau(j) = \tau(5+j) = \tau(5) + jl$$

in $\mathbb{F}_5$. This implies that $\tau \in \mathrm{AGL}(1,\mathbb{F}_5)$. So $N_{S_5}(\langle\theta\rangle) = \mathrm{AGL}(1,\mathbb{F}_5)$.

Now suppose that G contain more than one subgroup of order 5. Because $\langle(12345)\rangle$ is a 5-Sylow group, the third Sylow theorem indicates that the number of order 5 subgroups in G is congruent to 1, modulo 5, implying that G would contain at least $6 * 4 = 24$ distinct 5-cycles. But combinatorics shows that the number of distinct 5-cycles in S_5 is 24, so G must contain all of them.

The final part of proof goes: the identity

$$(ijklm)(ijmlk) = (ikj), \quad \{i,j,k,l,m\} = \{1,2,3,4,5\}$$

shows that G contain all the 3-cycles as well (same argument applies if the 3-cycle has form $(ij)(lm)$), so $A_5 \le G$. Therefore $G = S_5$ or A_5. □

5.2. **Classification of irreducible quintics when characteristic is not 2.** We first state the big theorem, then set out to find the sextic resolvent mentioned. When that's done, we'll come back and prove it.

Theorem 5.2. *Assume that $f \in F[x]$ is monic, separable, and irreducible of degree 5 and the characteristic of F is not 2, then the transitive subgroup $Gal(f) \simeq G \subset S_5$ has the following properties:*

(1) $G \subset A_5$ if and only if $\Delta(f) \in F^2$.
(2) G is conjugate to some subgroup of$AGL(1, \mathbb{F}_5)$ if and only if the sextic resolvent θ_f has a root in F.
(3) G is conjugate to $\langle(12345)\rangle$ if and only if f splits completely over $F(\alpha)$, where α is a root of f.

(1). This follows the theorem about discriminant mentioned previously. □

(3). This is left as an exercise. □

Here's a table to summarize the classification:

Is $\Delta(f)$ in F^2?	Does $\theta_f(y)$ have a root in F?	Does $f(x)$ split completely over $F(\alpha)$?	G up to conjugacy
No	No	—	S_5
Yes	No	—	A_5
No	Yes	—	$\mathrm{AGL}(1,\mathbb{F}_5)$
Yes	Yes	No	$\mathrm{AGL}(1,\mathbb{F}_5)\cap A_5$
Yes	Yes	Yes	$\langle(12345)\rangle$

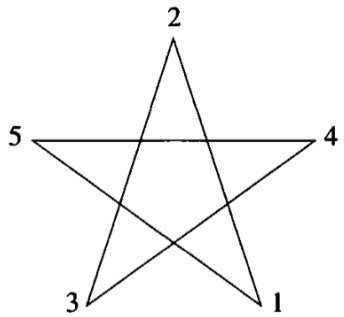
Now we'll define the sextic resolvent. But first of all, we want to find a polynomial $h \in F[x_1, x_2, x_3, x_4, x_5]$ such that

$$\{\tau \in S_5 | \tau \cdot h = h\} = \mathrm{AGL}(1, \mathbb{F}_5).$$

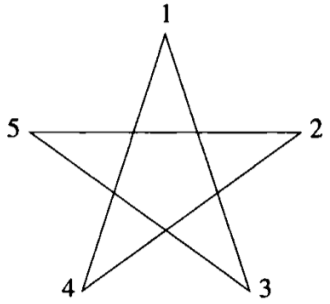
We'll use $h = u^2$ where

$$\begin{aligned} u \ &= x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 \\ &\quad - x_1x_3 - x_3x_5 - x_5x_2 - x_2x_4 - x_4x_1. \end{aligned}$$

Here's a graphical interpretation of definition of u, obtained by connecting x_i, x_j if the term x_ix_j has coefficient 1, and not connecting them if the term x_ix_j has coefficient -1.



Interpreted this way, (12345) is a rotation by one-fifth. It follows that $(1,2,3,4,5)\cdot u = u$. On the other hand, (1243) takes the above diagram to



Sharp eyed readers already spotted that here i, j are connected if and only if they are not connected previously. Thus $(1243)\cdot u = -u.$, and $h = u^2$ is fixed under $\mathrm{AGL}(1,\mathbb{F}_5)$.

By expanding out the formula to look at terms, it is clear that $G = \mathrm{AGL}(1,\mathbb{F}_5)$.

The left coset representation of $\mathrm{AGL}(1,\mathbb{F}_5)$ in S_5 are

$$e,\ (123),\ (234),\ (345),\ (145),\ (125). \tag{17}$$

So the orbit of S_5 acting on h consists of

$$h_1 = e\cdot h = h,\quad h_2 = (123)\cdot h,\quad h_3 = (234)\cdot h,$$
$$h_4 = (345)\cdot h,\quad h_5 = (145)\cdot h,\quad h_6 = (125)\cdot h.$$

Definition 18. Define the universal sextic resolvent be

$$\theta(y) = \prod_{i=1}^{6}(y - h_i).$$

Theorem 2.2.2 in Cox implies that $\theta(y)$ has coefficient in $F[\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5]$.

Now, consider the monic separable irreducible quintic be written as

$$f = x^5 - c_1x^4 + x_2x^3 - c_3x^2 + c_4x - c_5 \in F[x],$$

and let α_i, $i = 1,2,3,4,5$ be its roots in the splitting field. Then we know the evaluation map $x_i \mapsto \alpha_i$ would map $\sigma_i \mapsto c_i \in F$. Thus we can define the *sextic resolvent* for f be

$$\theta_f(y) = \prod_{i=1}^{6}(y - \beta_i) \in F[y]$$

where $\beta = h_i(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)$ in the splitting field.

Theorem 5.3. *The sextic resolvent can be written as*

$$\theta_f(y) = (y^3 + b_2y^2 + b_4y + b_6)^2 - 2^{10}\Delta(f)y,$$

where $b_2, b_4, b_6 \in F$.

We're not including a proof of theorem 3 here, interested reader should read the p374-375 on Cox.

proof of theorem 4.2 (2). First suppose that if G conjugate to some subgroup of $\mathrm{AGL}(1,\mathbb{F}_5)$, then relabel roots if necessary we can assume wlog $G \leq \mathrm{AGL}(1,\mathbb{F}_5)$. Let L be splitting field of f. Choose arbitrary $\sigma \in \mathrm{Gal}(f) = \mathrm{Aut}(L/F)$, and let it corresponds to some $\tau \in G$, then

$$\begin{aligned}\sigma(\beta_1) &= \sigma(h(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)) \\ &= h(\sigma(\alpha_1),\sigma(\alpha_2),\sigma(\alpha_3),\sigma(\alpha_4),\sigma(\alpha_5)) \\ &= (\tau\cdot h)(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5) \\ &= h(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5) = \beta_1.\end{aligned}$$

□

This shows that $\beta_1 \in F$ because extension L/F is Galois.

For the other direction, assume that θ_f has a root in F, but rather G is not conjugate to a subgroup of $\mathrm{AGL}(1,\mathbb{F}_5)$. Then by classification of transitive subgroups in S_5 we know $G = A_5$ or S_5. In particular it includes all 3-cycles. Let $\tau_1,...\tau_6 \in G$ be as defined in (12) and σ_i be corresponding element in $\mathrm{Gal}(f)$, then by arguing as above

$$\sigma_i(\beta_1) = \beta_i, \quad i = 1,...,6.$$

Because θ_f has a root in F, one of the $\beta_i \in F$. Using the fact that all of the three cycles are contained in G we get $\beta_1 = ... = \beta_6$, and we can write

$$\theta_f(y) = (y-\beta_1)^6$$

recalling that $\theta_f \in F(y)$ so its coefficients are invariant under σ. Comparing this with Theorem 4.3 to obtain the identity

$$(y-\beta_1)^6 = (y^3+b_2y^2+b_4y+b_6)^2 - 2^{10}\Delta(f)y. \tag{19}$$

Expand the coefficients for y^5, y^4, y^3 and solve for the equations give

$$b_2 = -3\beta_1, \;\; b_4 = 3\beta_1^2, \;\; b_6 = -\beta_1^3.$$

But this is absurd, because identity (14) now reads

$$(y-\beta_1)^6 = (y-\beta_1)^6 - 2^{10}\Delta(f)y,$$

implying that $\Delta(f) = 0$, contradicting our assumption that f is separable.

5.3. **Exercises.**

Excercise 20. Prove Lemma 12.

Proof. (1) → (2) orbit stablizer thm. (2) → (3) Cauchy theorem. (3) → (1) trivial. □

Excercise 21. Prove Lemma 14.

Proof. (a) $\mathrm{AGL}(1,\mathbb{F}_5)$ is generated by the translation $i \mapsto i+1$ - which is the five cycle (12345) and multiplication by 2: $i \mapsto 2i$, which corresponds to (1243).
(b) Easy to see that $[\mathrm{AGL}(1,\mathbb{F}_5) : \mathrm{AGL}(1,\mathbb{F}_5) \cap A_5] = 2$, so $|\mathrm{AGL}(1,\mathbb{F}_5) \cap A_5| = 10$. The only group of order 10 is $D_{10} \cong \mathbb{Z}_5 \times \mathbb{Z}_2$, so we can concludes the result.
(c) The order of a transitive subgroup of $\mathrm{AGL}(1,\mathbb{F}_5)$ is a multiple of 5 and a divisor of 20, the statement follows. □

Excercise 22. Prove Theorem 5.2(3)

Proof. By fundamental theorem of Galois theory, $[L : F] = |G| = 5$ where L is the splitting field of f. Because f of degree 5 is a minimal polynomial for any of its roots, L must be a simple extension. □

6. Kronecker's Analysis

Let F be an infinite field, and suppose $\alpha_1, \ldots, \alpha_n$ are the roots of f in the splitting field L/F. From Section 12.2 we know there are $t_1, \ldots t_n \in F$ such that

$$k(\sigma) = \sum_{=1}^{n} t_i \alpha_{\sigma(i)}, \quad \sigma \in \mathfrak{S}_n$$

are unique and there are $n!$ of them. Therefore,

$$s(y) = \prod_{\sigma \in \mathfrak{S}_n} (y - k(\sigma)) \in L[y]$$

is a separable polynomial of degree $n!$.

We know that from earlier in the book (Section 12.3) if $s(y) \in F[y]$ and $h(y) \in F[y]$ is an irreducible factor of $s(y)$, then $F[y]/(h(y))$ is the splitting field of f over f. Note the degree of $h(y)$ is equal to $[\mathrm{Gal}(f) : F]$.

We may generalize $s(y)$. First, let

$$k(x_1, x_2, \ldots, x_n, \sigma) = \sum_{=1}^{n} t_i x_{\sigma(i)}, \quad \sigma \in \mathfrak{S}_n$$

then define

$$S(y) = \prod_{\sigma \in \mathfrak{S}_n} (y - k(x_1, x_2, \ldots, x_n, \sigma)) \in F[x_1, \ldots, x_n, y].$$

We know how to write $S(y)$ as a polynomial in $F[x_1, \ldots, x_n, y]$, so once we specialize the coefficients to those of f, then we will recover $s(y)$. From Exercise 26 below, we know we can pick $t_i \in F$ so $s(y)$ is separable.

Example 23. Let $f = x^3 + xr - 2x - 1 \in [x]$, then from omitted calculations the universal polynomial will be

$$\begin{aligned} S(y) = {} & y^6 - 4\sigma_1 y^5 + (2\sigma_1^2 + 14\sigma_2)y^4 + (8\sigma_1^3 - 44\sigma_1\sigma_2 + 20\sigma_3)y^3 \\ & + (-7\sigma_1^4 + 18\sigma_1^2\sigma_2 + 49\sigma_2^2 - 40\sigma_1\sigma_3)y^2 + (-4\sigma_1^5 + 44\sigma_{12}^3 \\ & - 112\sigma_1\sigma_2^2 - 20\sigma_1^2\sigma_3 + 140\sigma_2\sigma_3)y + 4\sigma_1^6 - 32\sigma_1^4\sigma_2 + 55\sigma_1^2\sigma_2^2 \\ & + 36\sigma_2^3 + 76\sigma_1^3\sigma_3 - 322\sigma_1\sigma_2\sigma_3 + 343\sigma_3^2 \end{aligned}$$

Then using $\sigma_1 \mapsto -1$, $\sigma_2 \mapsto -2$, $\sigma_3 \mapsto 1$, we have

$$s(y) = (y^3 + 2y^2 - 15y + 13)(y^3 + 2y^2 - 15y - 29)$$

then $s(y)$ is separable. Hence, G_f over has order 3.

Other than just the order, using $s(y)$ we can find the entire Galois group from just an irreducible factor of $s(y)$.

Suppose $t_i \in F$ and let them be indeterminates, then define

$$s_t(y) = \prod_{\sigma \in \mathfrak{S}_n} (y - k(\sigma)) \in L[t_1, \ldots, t_n, y].$$

Then by Exercise 27, we know the coefficients are in F so $s_t(y) \in F[t_1, \ldots, t_n, y]$. Then, we can compute $s_t(y)$ by specializing to f after our generalization. Hence, we can find $s_t(y)$ without the roots of f. Note, that $F[t_1, \ldots, t_n, y]$ has an $\mathfrak{S}_n$ action that will permute the indeterminates, and that it is a unique factorization domain. For the splitting field of F, L, then the corresponding polynomial ring, $L[t_1, \ldots, t_n, y]$ will have the same properties as above, but also will have a $\mathrm{Gal}(L/F)$-action by the Galois action on L.

We can write the Galois group of f over F as $\mathrm{Gal}(L/F) \cong G_f \subseteq \mathfrak{S}_n$. Now we will state the main theorem,

Theorem 6.1. *Suppose $f \in F[x]$ is monic and separable of degree n, letting F be an arbitrary field. Furthermore, let $h \in F[t_1, \ldots, t_n, y]$ be an irreducible factor of $s_t(y) \in F[t_1, \ldots, t_n, y]$. Then $G_f \subseteq \mathfrak{S}_n$ is conjugate to the subgroup*

$$G = \{\sigma \in \mathfrak{S}_n \mid \sigma(h) = h\} \subseteq \mathfrak{S}_n$$

Proof. We know that the form we showed above of $s_t(y)$ is an irreducible factorization of the polynomial in $L[t_1, \ldots, t_n, y]$ from Exercise 28. Therefore, we can choose $\tau \in \mathfrak{S}_n$ so that

$$y - (k(\alpha_1, \ldots, \alpha_n, \tau))$$

is a factor of $h \in L[t_1, \ldots, t_n, y]$. We want to prove that $G = \tau^{-1} G_f \tau$. If we consider

$$\tilde{h} = \prod_{\gamma \in \mathrm{Gal}(L/F)} (y - k(\gamma(\alpha_1), \ldots \gamma(\alpha_n), \tau)) = \prod_{\mu \in G_f} (y - k(\alpha_1, \ldots, \alpha_n, \mu\tau)).$$

Note $\tilde{h}$ is invariant under the action of $\mathrm{Gal}(L/F)$ so we see $\tilde{h} \in F[t_1, \ldots, t_n, y]$ since $F \subseteq L$ is Galois. If we choose any $\mu \in \mathrm{Gal}(L/F)$, then since h has coefficients in F and divides h in $L[t_1, \ldots, t_n, y]$, we see

$$y - k(\gamma(\alpha_1), \ldots, \gamma(\alpha_n), \tau)$$

will divide $\gamma \cdot h = h$ in $L[t_1, \ldots, t_n, y]$. Thus, $\tilde{h} | h$ in $L[t_1, \ldots, t_n, y]$. From the exercise above, we know that $\tilde{h} | h$ in $F[t_1, \ldots, t_n, y]$ and since h is irreducible we know that $\tilde{h} = h$ after multiplication of h by some constant.

Now if we consider some $\varrho \in \mathfrak{S}_n$ since $\varrho \cdot h = h$, then this implies that that $\varrho \cdot (y - (k(\alpha_1, \ldots, \alpha_n, \tau)))$ will be a factor of h in $L[t_1, \ldots, t_n, y]$. Then since $\tilde{h}$ is the irreducible factorization of h in $L[t_1, \ldots, t_n, y]$, we find,

$$y - \sum_{i=1}^{n} t_{\varrho(i)} \alpha_{\tau(i)} = y - k(\alpha_1, \ldots, \alpha_n, \mu\tau)$$

for some $\mu \in G_f$. Since each t_i is distinct, we find,

$$\varrho(i) = j \implies \alpha_{\tau(i)} = \alpha_{\mu\sigma(j)} \implies \alpha_{\tau\varrho^{-1}(j) = \alpha_{\mu\tau(j)}}$$

therefore, $\tau\varrho^{-1} = \mu\tau$, and since $\alpha_1, \ldots, \alpha_n$ are distinct so

$$\varrho = \tau^{-1}\mu^{-1}\tau \in \tau^{-1}G_f\tau$$

so $G \subseteq \tau^{-1}G_f\tau$. For the other direction, you will prove it in the Exercise 28. □

Example 24. If $f = x^3 - 1 \in [x]$, then from Exercise 29,

$$\begin{aligned} s_t(y) = &(y^2 + (u_1 + u_2 - 2u_3)y + u_1^2 + u_2^2 + u_3^2 - u_1u_2 - u_1u_3 - u_2u_3) \\ &\cdot (y^2 + (u_1 + u_3 - 2u_2)y + u_1^2 + u_2^2 + u_3^2 - u_1u_2 - u_1u_3 - u_2u_3) \\ &\cdot (y^2 + (u_2 + u_3 - 2u_1)y + u_1^2 + u_2^2 + u_3^2 - u_1u_2 - u_1u_3 - u_2u_3) \end{aligned}$$

In each factor, the terms of degree 0 are symmetric in u_1, u_2, u_3. From this it follows that the first factor will be $G = \langle(12)\rangle$, second term $G = \langle(13)\rangle$ and the third will be $G = \langle(23)\rangle$.

Corollary 25. Suppose R is a unique factorization domain, $\mathfrak{p}$ is a prime ideal in R, $k = \mathrm{Frac}(R)$, and $k_\mathfrak{p} = \mathrm{Frac}(R/\mathfrak{p})$. Then let $f \in R[x]$ be a monic polynomial, then denote by $f_\mathfrak{p}(x)$ the coset of $f(x)$ in $R/\mathfrak{p}[x]$. If both f and $f_\mathfrak{p}$ are separable, then the Galois group of the splitting field $K_\mathfrak{p}$ of $f_\mathfrak{p}$ over $k_\mathfrak{p}$ is a subgroup of the Galois group of the splitting field K of $f(x)$ over k. [3]

Proof. If $z \in L[t_1, \ldots, t_n, y]$ as above. Then since Kronecker's theorem on symmetric polynomials holds over a ring we find $z \in R[t_1, \ldots, t_n, y]$. We can also make the polynomial $z_\mathfrak{p}(t_1, \ldots, t_n, y)$ where it can be formed in two ways. First, from f_p and also by taking the coset of z in $R/\mathfrak{p}[t_1, \ldots, t_n, y]$. Both of these constructions form the same $z_\mathfrak{p}$.

Since R is a UFD, we know there is no difference between the factorization of polynomials with coefficients in R in the ring $R[t_1, \ldots, t_n, y]$ and $k[t_1, \ldots, t_n, y]$ by Gauss' Lemma. Over $R/\mathfrak{p}$, the polynomial $h \in R[t_1, \ldots, t_n, y]$ may be reducible and modulo $\mathfrak{p}$ we will deal with the permutations preserving of one irreducible factor of $z_\mathfrak{p}$ only.

From the theorem above, we can infer that a permutation preserving one irreducible factor of z will preserve each of them and this shows $\mathrm{Gal}(K_\mathfrak{p}/k_\mathfrak{p}) \subseteq \mathrm{Gal}(K/k)$ as desired. □

6.1. **Exercises.**

Excercise 26. (1) Prove that if f is separable, then $\Delta(s)$ is a nonzero polynomial if t_i are considered variables.
(2) Show that $\Delta(s) \neq 0$ for some $t_i \in \mathbb{Z}$.
(3) Show finally that we can pick $t_i \in F$ so $s(y)$ is separable without knowing its roots.

Excercise 27. Prove $s_t(y)$ is in $F[t_1, \ldots, t_n, y]$

Excercise 28. (1) Let $\beta_i \in L$ for $0 < i \leq n$, then prove $y + \sum_{i=1}^n \beta_i u_i$ is irreducible in $L[u_1, \ldots, u_n, y]$
(2) Let $g, h \in F[u_1, \ldots, u_n, y]$ and assume that in $L[u_1, \ldots, u_n, y]$, $h = gq$ for some $q \in L[u_1, \ldots, u_n, y]$. Then prove $q \in F[u_1, \ldots, u_n, y]$.
(3) Prove that $\tau^{-1}G_f\tau \subseteq G$.

Excercise 29. Compute the factorization of $s_t(y)$ from Example 24 above using the method from Exercise 4 in the book [2].

References

[1] V. Arvind and Piyush P. Kurur. Upper bounds on the complexity of some galois theory problems. In Toshihide Ibaraki, Naoki Katoh, and Hirotaka Ono, editors, *Algorithms and Computation*, pages 716–725, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[2] D.A. Cox. *Galois Theory*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2004.

[3] Vladimir Dotsenko. *Notes for Module 3419, "Galois Theory"*.