MATH411-21S2 GALOIS THEORY LECTURE NOTES

Contents

1. Introduction

Galois theory is named after Evariste Galois (1811-1832). The roots of a polynomial $f(x) \in k[x]$ over a field k have symmetries which form a group. Galois theory studies such groups and how they can be used to describe the structure of the splitting field of $f(x)$ over k. The goal of this course is to develop this theory (and the necessary group theory) and use this to prove the following two theorems:

Theorem 1.1 (Rufini 1799, Abel 1824)**.** *A general polynomial of degree at least 5 has no solution in radicals*

Theorem 1.2 (Fundamental Theorem of Algebra)**.** *Every nonconstant polynomial over the complex numbers has a root.*

Along the way we will need to learn a fair amount of group theory.

Theorem 1.3 (Quadratic formula)**.** *The roots of* $f(x) = x^2 + ax + b \in \mathbb{Q}[x]$ *are given by* $x = \frac{a \pm \sqrt{a^2-4b}}{2}$

Corollary 1.4. *All quadratic extensions of* $\mathbb{Q}$ *are of the form* $\mathbb{Q}(\sqrt{d})$ *for some* $d \in \mathbb{Q}$*.*

Theorem 1.5 (Cubic Formula, 1500's)**.** *Let* $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ *and set*

$$\Delta_1 = \dots$$

Corollary 1.6. *Any cubic polynomial* $f(x) \in \mathbb{Q}[x]$ *splits in a field* K *of the form*

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{d}) = K_1 \subset K_1(\sqrt[3]{e}) = K$$

where $d \in \mathbb{Q}$ *and* $e \in K_1$

Definition 1.7. *We say $K/\mathbb{Q}$ is a radical extension if K is obtained by a sequence of extensions of the form*

$$\mathbb{Q} = K_1 \subset K_1(\sqrt[n_1]{a_1}) = K_2 \subset K_2(\sqrt[n_2]{a_2}) = K_3 \cdots K_m(\sqrt[n_m]{a_m}) = K$$

for some $a_i \in K_i$ and $n_i \in \mathbb{Z}_{\geqslant 2}$.

The quadratic and cubic formulas above show that every degree 2 or 3 polynomial splits over a radical extension. This means you can give a formula for the roots of the polynomial which only require n-th roots and the usual arithmetic operations. There is also a quartic formula (Ferrari 1540) which shows that the same is true for degree 4 polynomials. The Abel-Rufini theorem mentioned above states that a general quintic polynomial does not split over any radical extension. Galois theory gives a characterization of the polynomials that split in a radical extension by looking at the group of symmetries of the roots (a concept that we will cover in more depth later).

Here is a sketch of the idea: The roots of a polynomial have symmetries. These symmetries form a group, called the Galois group of the polynomial. For example the roots $x = \frac{a \pm \sqrt{a^2-4b}}{2}$ of $f(x) = x^2 + ax + b$ have a symmetry encoded in the $\pm$. The corresponding group is $\mu_2 = \{\pm 1\}$ under multiplication. More generally, the n-th roots of an element of a field have symmetries described by a group μ_n. Consequently polynomials that split in radical extensions have Galois groups that are of a rather particular type (called solvable groups). Galois proved that there are groups which are not solvable (for example the alternating group A_5) and moreover that there are quintic polynomials which have such nonsolvable groups as their Galois groups. Such polynomials cannot possibly split in any radical extension.

2. Galois theory – first examples

Let F be a field and $f \in F[x]$ a polynomial with coefficients in F. Let E be the splitting field of f, i.e., the minimal extension of F over which f splits into linear factors.

Definition 2.1. *The Galois group of f is*

$$\mathrm{Gal}(f) = \mathrm{Aut}(E|F) = \{\phi : E \to E \ : \ \phi \text{ is an isomorphism and } \phi(a) = a \text{ for all } a \in F\}.$$

By definition there is an action of $\mathrm{Gal}(f)$ on E. It is not difficult to prove the following:

Lemma 2.2. *Suppose f factors over E as $f = (x-\theta_1)\cdots(x-\theta_n)$. Then the action of $\mathrm{Gal}(f)$ on E restricts to an action on $\{\theta_1, \ldots, \theta_n\}$. This yields an injective homomorphism $\mathrm{Gal}(f) \hookrightarrow \mathrm{Sym}\{\theta_1, \ldots, \theta_n\} \simeq S_n$. Moreover, if f is irreducible (over F), then the image is a transitive subgroup of S_n.*

Example 1: Suppose $f(x) = x^2 - d$ with $d \in F$ not a square and F not of characteristic 2.

Since d is not a square f is irreducible and the splitting field of f is $E = F[x]/\langle f(x)\rangle = F[\theta]$, where θ is the image of x in E (You should think $\theta = \sqrt{d}$). Then $E = \{a + b\theta \ : \ a, b \in F\}$ is a 2-dimensional vector space over F, with multiplication given using $\theta^2 = d$.

Over E, f factors as $f = (x-\theta)(x-(-\theta)) = (x-\theta_1)(x-\theta_2)$, with $\theta_1 = \theta$ and $\theta_2 = -\theta$. The map $\theta \mapsto -\theta$ extends to the isomorphism $\phi_{-1} : E \to E$ sending $a + b\theta$ to $a - b\theta$. This gives a nontrivial element of $\mathrm{Gal}(f) = \mathrm{Aut}(E|F)$. Since $\mathrm{Gal}(f) \hookrightarrow S_2 \simeq \{\pm 1\}$, we see $\mathrm{Gal}(f) = \{\phi_1, \phi_{-1}\}$, where ϕ_{-1} is the identity.

What can we recover from the actions $\mathrm{Gal}(f) \circlearrowright E$ and $\mathrm{Gal}(f) \circlearrowright \{\theta_1, \theta_2\}$?

For one, F is the fixed subset of $G \circlearrowright E$, i.e., $F = E^G := \{e \in E \ : \ \forall\, \phi \in G\,,\ \phi(e) = e\,\}$. Another way to express this is that the stablizer of an element determines whether or not it lies in F. Specifically, for $\alpha \in E$ we have $\mathrm{Stab}(\alpha) = \begin{cases} G & \alpha \in F \\ 1 & \alpha \in E \backslash F\,. \end{cases}$

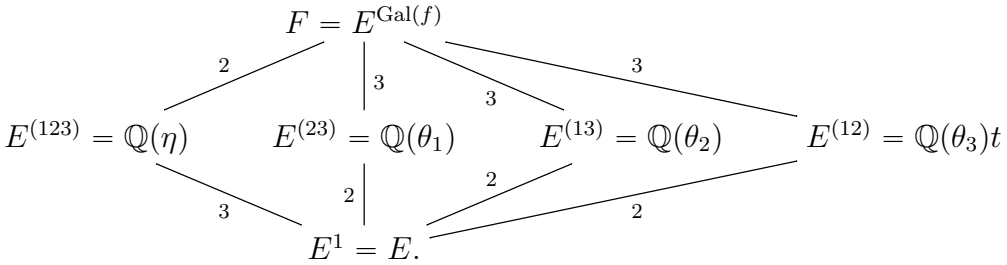
From the action of $\mathrm{Gal}(f)$ on the roots of f we can recover (up to sign) the characteristic polynomial of any element, i.e., the characteristic polynomial of the linear map of the F-vector space $L_\beta : E \to E$ given by $\alpha \mapsto \beta\alpha$. When $\beta \in E \backslash F$ this is the same as the minimal polynomial of β. For example, f is the minimal polynomial of θ and we can recover it as $f = \prod_{\phi \in G}(x - \phi(\theta)) = (x - \theta)(x + \theta) = x^2 - d$. More generally, if $\beta = a + b\theta$, then $\chi_\beta(x) := \prod_{\phi \in G}(x - \phi(\beta)) = (x - (a + b\theta))(x - (a - b\theta)) = x^2 - 2a + (a^2 - b^2\theta^2) = x^2 - 2a + (a^2 - db^2) \in F[x]$. This is a monic polynomial of degree 2 with coefficients in F that clearly has β as a root. If $\beta \in E \backslash F$, then it is the minimal polynomial. If $\beta \in F$, then $b = 0$ and $\chi_\beta(x) = (x - \beta)^2$. This is the characteristic polynomial of the F-linear map $E \to E$ given by $\alpha \mapsto a\alpha$. Indeed, with respect to the basis $\{1, \theta\}$ for E/F the matrix of the linear map is $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ which has characteristic polynomial $\det(\lambda I - aI) = (\lambda - a)^2$.

Example 2: Suppose $f(x) = x^3 - d$ with $d \in \mathbb{Q}$ not a cube.

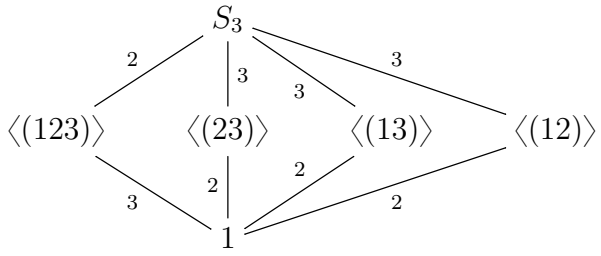
The splitting field of f is $E = \mathbb{Q}[\theta, \eta]$, where θ is a root of f and η is a root of $x^2 + x + 1$. Note that η is a primitive cube root of unity (i.e., $\eta^3 = 1$ but no smaller positive power of η is equal to 1). Over E we have $f = (x - \theta_1)(x - \theta_2)(x - \theta_3)$ where $\theta_1 = \theta$, $\theta_2 = \eta\theta$ and $\theta_3 = \eta^2\theta$. To construct E you would first construct $E_1 = \mathbb{Q}[\theta] = \mathbb{Q}[x]/\langle f \rangle$ and then factor $f = (x - \theta)(x^2 + \theta x + \theta^2)$ over E_1. Then $E = E_1[x]/\langle g \rangle$ where $g = x^2 + \theta x + \theta^2$. Over E, g factors as $g = (x - \eta\theta)(x - \eta^2\theta)$.

Now we compute $\mathrm{Gal}(f) = \mathrm{Aut}(E|\mathbb{Q})$. It is a transitive subgroup of S_3, so it contains (21) or (321) as there must be an element sending θ_1 to θ_2. Also it is clear from the definition that $\mathrm{Aut}(E|E_1) < \mathrm{Aut}(E|\mathbb{Q})$. By the example above, $\mathrm{Aut}(E|E_1) \simeq S_2$ which interchanges $\theta_2 = \eta\theta$ and $\theta_3 = \eta^2\theta$. The generator of this subgroup must leave $\theta_1 = \theta$ fixed since $\theta \in E_1$. Therefore $\mathrm{Gal}(f) < S_3$ also contains (23). It follows that $\mathrm{Gal}(f) \simeq S_3$.

For any subgroup $H < \mathrm{Gal}(f) = \mathrm{Aut}(E|\mathbb{Q})$ we can look at the fixed subfield:



There are in fact no other intermediate fields $\mathbb{Q} \subset M \subset E$, so the subfield lattice of $E/\mathbb{Q}$ looks just like the subgroup lattice of S_3 (with inclusions reversed). The 2's and 3's appearing on the edges are the degrees of the extensions. Note that these correspond to indices of subgroups in the correspond subgroup lattice.



This is called the Galois correspondence. Note also that the fields $\mathbb{Q}(\theta_i)$ are all isomorphic to $E_1 = \mathbb{Q}[x]/\langle f\rangle$, but are distinct as subfields of E. This corresponds to the fact that the corresponding subgroups are all conjugate.

The correspondence also goes the other way. For example, the subgroups $\mathrm{Aut}(E|F) \simeq S_3$ can be read off from the subfields of E. For example

$$\langle(123)\rangle = \{\phi \in \mathrm{Aut}(E|F) \ : \ \phi(\alpha) = \alpha \text{ for all } \alpha \in \mathbb{Q}(\eta)\}\,.$$

Indeed, none of the relfections in S_3 fix η, but $\phi_{(123)}$ does since

$$\phi_{(123)}(\eta) = \phi_{(123)}(\eta\theta/\theta) = \phi_{(123)}(\theta_2/\theta_1) = \theta_1/\theta_3 = \eta^{-2} = \eta\,.$$

Example 3: Consider $f = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$. I claim this splits over $E = \mathbb{Q}[x]/\langle f\rangle = \mathbb{Q}[\theta]$, as $f = (x-\theta_1)(x-\theta_2)(x-\theta_3)$ where

$$\begin{aligned}\theta_1 &= \theta\\ \theta_2 &= -\theta^2 - \theta + 1\\ \theta_3 &= \theta^2 - 2\,.\end{aligned}$$

Now suppose $\phi \in \mathrm{Gal}(f)$. Since each θ_i is a polynomial in θ_1, the action of ϕ on θ_2 and θ_3 is determined by its action on θ_1. For example, if $\phi(\theta_1) = \theta_2$, then $\phi(\theta_2) = \phi(-\theta_1^2 - \theta_1 + 1) = -\theta_2^2 - \theta_2 + 1 = \cdots = \theta_3$. Since $\mathrm{Gal}(f)$ is a transitive subgroup of S_3 it must be equal to the subgroup generated by some (hence any) 3-cycle. Note that $\mathrm{Gal}(f)$ has no proper subgroups and there are no proper intermediate fields $F \subset M \subset E$.

3. Galois extensions

Definition 3.1. *Let E/F be an algebraic extension. We say E/F is*

1. *separable if for every $\alpha \in E$, the roots of the minimal polynomial $f_\alpha \in F[x]$ are all distinct (in some/any splitting field).*
2. *normal if for every $\alpha \in E$, the minimal polynomial $f_\alpha \in F[x]$ splits over E.*
3. *Galois if $E^{\mathrm{Aut}(E|F)} = F$.*

The following theorem characterizes Galois extensions.

Theorem 3.2. *Let E/F be a an extension of fields. The following are equivalent.*

1. *E/F is a finite Galois extension;*
2. *$F = E^G$ for some finite group of automorphisms of E;*
3. *E is the splitting field over F of a separable polynomial $f \in F[x]$;*

(4) E/F is separable, normal and of finite degree.

The proof will occupy the rest of this section.

Example 3.3.
$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ *is separable and normal and Galois.*
$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ *is separable but not normal. It is also not Galois becuase* $\mathrm{Aut}(\mathbb{Q}\sqrt[3]{2})|\mathbb{Q}) = 1$*, so the fixed field is* $\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$.
$\mathbb{F}_2(\sqrt{t})/\mathbb{F}_2(t)$ *is normal, but not separable; it is the splitting field of* $x^2 - t = (x - \sqrt{t})^2$*. Again* $\mathrm{Aut}(\mathbb{F}_2(\sqrt{t})|\mathbb{F}_2(t)) = 1$ *so this is not Galois.*

Lemma 3.4. *Let $f \in F[x]$ be an irreducible polynomial, α a root of f and $\phi_0 : F \to E$ a field homomorphism. There is a one to one correspondence between the set*

$$\{\phi : F[\alpha] \to E \ : \ \phi = \phi_0 \text{ on } F\}$$

and the set of roots of the polynomial $\phi(f)$ in E.

Proof. For a polynomial $g = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$ let $\phi(g) = \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n$.

Given a root γ of $\phi(f)$ in E, consider the map $\psi : F[x] \to E$ sending g to $\phi(g)(\gamma)$. This is a homomorphism of rings with kernel $\{g \in F[x] \ : \ \phi(g)(\gamma) = 0\}$. This kernel contains f, but f is irreducible so it must generate the kernel. By the homomorphism theorem (for rings) ψ factors through an isomorphism $\phi : F[x]/\langle f \rangle = F[\alpha] \to E$. On the other hand, any map $F[\alpha] \to E$ which agrees with ϕ on F must send α to a root of $\phi(f)$. Indeed, since $0 = \phi(0) = \phi(f(\alpha)) = \phi(f)(\phi(\alpha))$. □

Proposition 3.5. *Let E be the splitting field of $f \in F[x]$. Then*

$$\#\,\mathrm{Aut}(E|F) \leqslant [E : F]$$

with equality if the roots of f are distinct.

Proof. We write $A \preceq B$ to mean $A \leqslant B$ with equality if the roots of f are distinct.

Let $\alpha_1, \ldots, \alpha_n \in E$ be the roots of f and let $F_i = F[\alpha_1, \ldots, \alpha_i]$ for $i = 0, \ldots, n$ (we take $F_0 = F$). We will show by induction that the number of field homomorphisms $F_i \to E$ that are the identity on F is $\preceq [F_i : F]$. The proposition is the case $i = n$.

The base of induction is $i = 0$; there is exactly 1 homomorphism $F \to F$ that is the identity on F and $[F : F] = 1$. So the statement holds.

Now suppose the statement holds for some $i \geqslant 0$. If $\phi : F_{i+1} \to E$ is a homomorphism that is the identity on F, the induction hypothesis gives that there are $\preceq [F_i : F]$ possibilities for the restriction of ϕ to F_i. We show that there are $\preceq [F_{i+1} : F_i]$ distinct ϕ's with the same restriction. Then in total there are $\preceq [F_{i+1} : F_i][F_i : F] = [F_{i+1} : F]$ possibilities for ϕ.

Let $f_{i+1} \in F_i[x]$ be the minimal polynomial of α_{i+1} over F_i. Note that f_{i+1} must divide the minimal polynomial of α_{i+1} over F, which divides f. So f_{i+1} must split over E and its roots will be distinct if the roots of f are distinct. By the lemma, the number of extensions of some $\phi_i : F_i \to E$ to a morphism $\phi_{i+1} : F_{i+1} \to E$ is equal to the number of roots of f_{i+1} in E. This number is $\preceq \deg(f_{i+1}) = [F_{i+1} : F_i]$. □

Theorem 3.6 (Artin's Lemma)**.** *Let G be a finite group of automorphisms of a field E. Then $[E : E^G] \leqslant \#G$.*

Proof. Let $G = \{\sigma_1, \ldots, \sigma_m\}$ and $\alpha_1, \ldots, \alpha_n \in E$ with $n > m$. Consider the system of equations over E:

$$\begin{aligned} \sigma_1(\alpha_1)X_1 + \cdots + \sigma_1(\alpha_n)X_n &= 0 \\ &\vdots \\ \sigma_m(\alpha_1)X_1 + \cdots + \sigma_m(\alpha_n)X_n &= 0\,. \end{aligned}$$

Or $A\mathbf{x} = \mathbf{0}$ where $A = [\sigma_i(\alpha_j)]$. The rank of A is at most m, which is less than n so there is a nontrivial solution in E^n. Let $\overline{c} = (c_1, \ldots, c_n) \in E^n$ be a nontrivial solution with as few nonzero entries as possible. Relabing if necessary we may assume $c_1 \neq 0$. We may then scale so that $c_1 = 1 \in E^G$. We claim that with this normalization $c_i \in F = E^G$ for all $i = 1, \ldots, n$. If $c_i \notin F$, then there is some $\sigma_k \in G$ such that $\sigma_k(c_i) \neq c_i$. Note that $\sigma_k(A) = [\sigma_k\sigma_i(\alpha_j)]$ differs from A by a permutation of the rows (since $G = \{\sigma_k\sigma_1, \ldots, \sigma_k\sigma_m\}$). In particular $\sigma_k(A)$ and A have the same nullspace. Now $\mathbf{0} = \sigma_k(\mathbf{0}) = \sigma_k(A\mathbf{c}) = \sigma_k(A)\sigma_k(\mathbf{c})$ shows that $\sigma_k(\mathbf{c})$ lies in the nullspace of $\sigma_k(A)$. Hence $\sigma_k(\mathbf{c})$ is a nontrivial solution and so $\overline{c} - \sigma_k(\overline{c})$ is as well. However, $\overline{c} - \sigma_k(\overline{c})$ is nonzero (the i-th entry is nonzero) and has fewer nonzero entries than $\overline{c}$ (since the 1-st entry is now 0). This contradicts our assumption thus proving that all c_i are in $F = E^G$.

Now consider the equation in the system with $\sigma_i = 1$. This equation is a linear dependence among the α_j with coefficients in $F = E^G$. Hence $[E : E^G] \leqslant m$. □

Proof of Theorem 3.2. We prove (4) ⇒ (3) ⇒ (2) ⇒ (1) ⇒ (4).

(4) ⇒ (3): Let $\alpha_1, \ldots, \alpha_n$ be a basis for E/F and let $g_i \in F[x]$ be the minimal polynomial of α_i. Let g be the product of the distinct polynomials in the list $g_1, \ldots, g_n$. Then g is a separable polynomial and E is its splitting field over F.

(3) ⇒ (2): Suppose E is the splitting field over F of the separable polynomial $f \in F[x]$ and set $G = \mathrm{Aut}(E|F)$. Then E is also the splitting field over E^G of $f \in E^G[x]$. Then

$$[E : E^G] \overset{(i)}{\leqslant} \#G \overset{(ii)}{\leqslant} \#\,\mathrm{Aut}(E|E^G) \overset{(iii)}{=} [E : E^G]$$

because (i) follows Artin's lemma and (ii) follows from $G < \mathrm{Aut}(E|E^G)$ and (iii) follows from the Proposition applied to $f \in E^G[x]$.

Using the Proposition applied to $f(x) \in F[x]$ and the above inequalities, it follows that $[E : F] = \#G = \#\,\mathrm{Aut}(E|E^G) = [E : E^G]$.

Since $F \subset E^G$ this implies $F = E^G$.

(2) ⇒ (1): Suppose $F = E^G$. Then $G < \mathrm{Aut}(E|F)$ so

$$F \subset E^{\mathrm{Aut}(E|F)} \subset E^G = F\,,$$

and $[E : F] \leqslant \#G < \infty$ by Artin's Lemma.

(1) ⇒ (4): Assume $F = E^{\mathrm{Aut}(E|F)}$ and $[E : F]$ is finite. We show E/F is separable and normal. Since E/F is finite every $\alpha \in E$ is algebraic over F. It suffices to show that the minimal polynomial $g_\alpha \in F[x]$ splits into distinct linear factors over E. Note that the orbit of α under the action of $\mathrm{Aut}(E|F)$ consists of roots of g_α and is in particular finite. So $\mathrm{Aut}(E|F)/\,\mathrm{Stab}(\alpha)$ is finite. Consider the polynomial $p = \prod_{\phi \in \mathrm{Aut}(E|F)/\,\mathrm{Stab}(\alpha)}(x - \phi(\alpha))$, where the product runs over a set of coset representatives for the stabiliser of the action of $\mathrm{Aut}(E|F)$ on $\alpha \in E$. Then

- p does not depend on the choice of coset representatives: if $\phi' = \phi \circ s$ for some $s \in \mathrm{Stab}(\alpha)$, then $\phi'(\alpha) = \phi(\alpha)$.
- p is separable: if p has a repeated root, then $\phi(\alpha) = \phi'(\alpha)$ for some $\phi \neq \phi'$ appearing in the product. But then $\phi^{-1}\phi = s \in \mathrm{Stab}(\alpha)$ so $\phi' = \phi \circ s$ and ϕ, ϕ' represent the same coset of $\mathrm{Stab}(\alpha)$.
- $p \in F[x]$: Let $\psi \in \mathrm{Aut}(E|F)$. Under the action $\mathrm{Aut}(E|F) \curvearrowright \mathrm{Aut}(E|F)/\mathrm{Stab}(\alpha)$ the effect of ψ is to permute the cosets. If $\phi_1, \ldots, \phi_n$ are representatives for the cosets, then so are $\psi\phi_1, \ldots, \psi\phi_n$. It follows that $\psi(p) = \prod(x - \phi_i(\alpha)) = \prod(x - \psi\phi_i(\alpha)) = p$. This shows that all coefficients of p are fixed by ψ. Since ψ is arbitrary we conclude that the coefficients of p lie in $E^{\mathrm{Aut}(E|F)} = F$.

Since α is clearly a root of $p \in F[x]$ we must have that $g_\alpha \mid p$ (the minimal polynomial of α divides any polynomial which has α as a root). Since p splits into distinct linear factors over E, g_α must as well. □

Example 3.7. *The following example may help to clarify the proof of* (1) ⇒ (4) *above. Consider* $E = \mathbb{Q}(\theta, \eta)$ *where* $\theta^3 = 2$, $\eta^3 = 1$, $\eta \neq 1$. *Then* $\mathrm{Aut}(E|F) \simeq \mathrm{Sym}\{\alpha_i = \eta^i\theta\} \simeq S_3$. *Let's carry out the proof for* $\alpha = \theta$. *Then* $\mathrm{Stab}(\alpha)$ *is generatred by the transposition* $(1\,2)$ *swaping* $\eta\theta$ *and* $\eta^2\theta$. *A set of coset representatives for* $\mathrm{Stab}(\alpha)$ *is given by* $\phi_1 = 1, \phi_2 = (1\,3)$ *and* $\phi_3 = (2\,3)$. *We form* p *as:*

$$p = (x - \phi_1(\theta))(x - \phi_2(\theta))(x - \phi_3(\theta)) = (x - \theta)(x - \eta\theta)(x - \eta^2\theta) = x^3 - 2\,.$$

Let's check the claim that $\psi(p) = p$ *for* $\psi = (123)$ *(This was used to prove the coefficients of* p *lie in* F*). We have*

$$\psi(p) = (x - \psi \circ \phi_1(\theta))(x - \psi \circ \phi_2(\theta))(x - \psi \circ \phi_3(\theta)) = (x - \eta^2\theta)(x - \theta)(x - \eta\theta) = p\,.$$

4. The Galois Correspondence

Theorem 4.1. *Let* E/F *be a finite Galois extension. There is a one-to-one correspondence between the set of intermediate fields* $F \subset M \subset E$ *and the set of subgroups* $H < \mathrm{Aut}(E|F)$ *given by*

$$\Phi\colon M \mapsto H_M := \mathrm{Aut}(E|M) < \mathrm{Aut}(E|F)\,,$$
$$\Psi\colon H \mapsto E^H := \{\alpha \in E \ :\ \forall\, \phi \in H\,,\ \phi(\alpha) = \alpha\}\,.$$

Moreover,

(1) (inclusion reversing) $H_1 \supset H_2 \Leftrightarrow E^{H_1} \subset E^{H_2}$;
(2) (indicies equal degrees) $[H_1 : H_2] = [E^{H_2} : E^{H_1}]$;
(3) $E^{\phi H \phi^{-1}} = \phi(E^H)$ *and* $H_{\phi(M)} = \phi H_M \phi^{-1}$;
(4) M/F *is Galois if and only if* $H_M \lhd \mathrm{Aut}(E|F)$, *in which case* $\mathrm{Aut}(M/F) \simeq \mathrm{Aut}(E|F)/H_M$.

Proof. One easily checks that H_M is a subgroup of $\mathrm{Aut}(E|F)$ and E^H is a subfield of E containing F. To prove the correspondence is one-to-one, we check that Φ and Ψ are inverse to one another.

Let $H < \mathrm{Aut}(E|F)$. Then E/E^H is a Galois extension since it satisfies (2) of Theorem 3.2 and $\Phi(\Psi(H)) = \mathrm{Aut}(E|E^H) = H$ (by the proof of (2) ⇒ (1) of that theorem). So $\Phi \circ \Psi$ is the identity map on the set of subgroups of $\mathrm{Aut}(E|F)$. Let M be an intermediate field. Since E/F is Galois, E is the splitting field of some separable polynomial $f \in F[x]$ by Theorem 3.2.

Then E/M is the splitting field of the separable polynomial $f \in M[x]$. Hence E/M is Galois which means that $\Psi(\Phi(M)) = E^{=} E^{\mathrm{Aut}(E|M)} = M$. In other words $\Psi \circ \Phi$ is the identity map.

(1) That the correspondence reverses inclusions is obvious.

(2) For any $H < \mathrm{Aut}(E|F)$ we have E/E^H is Galois. and so $[H : 1] = \#H = \#\,\mathrm{Aut}(E|E^H) = [E : E^H]$. Applying this with $H = H_1$ and $H = H_2$ we see

$$[H_1 : H_2] = \frac{[H_1 : 1]}{[H_2 : 1]} = \frac{[E : E^{H_1}]}{[E : E^{H_2}]} = [E^{H_2} : E^{H_1}]\,.$$

(3) Let $a, b \in E, b = \phi^{-1}(a)$. For any $\tau \in \mathrm{Aut}(E|F)$, let $\sigma = \phi\tau\phi^{-1}$. Then $\sigma(a) = \phi\tau(b)$, so $\sigma(a) = a$ if and only if $\tau(b) = b$. This shows that $a \in E^{\phi H \phi^{-1}}$ if and only if $b \in E^H$, i.e $a \in \phi(E^H)$, so $E^{\phi H \phi^{-1}} = \phi(E^H)$ and the other equality is similar.

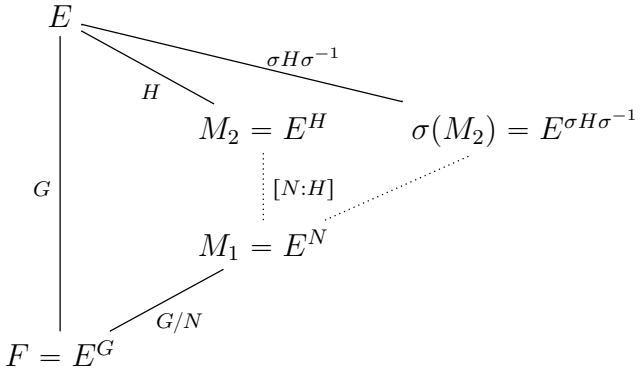
(4) First suppose M/F is Galois. Then it is normal by Theorem 3.2. If $\alpha \in M$ and $\phi \in \mathrm{Aut}(E|F)$, then $\phi(\alpha)$ is a root of the minimal polynomial of α hence lies in M. This shows that $\phi(M) = M$. By (3) this means that $H_M = H_{\phi(M)} = \phi H_M \phi^{-1}$, so H_M is normal.

Conversely, if H_M is normal, then (3) shows that $\phi(M) = M$ for any $\phi \in \mathrm{Aut}(E|F)$. Thus, any element of $\mathrm{Aut}(E|F)$ restricts to an automorphism of M. This defines a homomorphism $\mathrm{Aut}(E|F) \to \mathrm{Aut}(M|F)$. Let H be the image. Then $M^H \subset E^{\mathrm{Aut}(E|F)} = F$ and, in particular, $M^{\mathrm{Aut}(M|F)} = F$ is M/F is Galois.

Moreover, this homomorphism is surjective by (2) (the image has size $[\mathrm{Aut}(E|F) : H_M] = [M : F] = [\mathrm{Aut}(M|F) : 1]$. Then $\mathrm{Aut}(E|F)/H_M \simeq \mathrm{Aut}(M|F)$ by the homomorphism theorem.

□

The following diagram summarizes the general picture for $G = \mathrm{Gal}(E|F)$ and subgroups $H < N \lhd G$.



The solid lines correspond to Galois extensions with the indicated Galois group. The dashed line indicates that the extension may not be Galois, but has the indicated degree.

Example: Consider the example $E = \mathbb{Q}(\theta, \eta)$, $\theta^3 = 2$, $\eta^2 + \eta + 1 = 0$, with $\mathrm{Aut}(E|\mathbb{Q}) = \mathrm{Sym}\{\eta^i\theta\} \simeq S_3$. The only proper normal subgroup is $H = \langle \phi_{(123)} \rangle$. The fixed field is $\mathbb{Q}(\eta) = E^H$. Over $\mathbb{Q}(\eta)$, the minimal polynomial $f_\eta = x^2 + x + 1$ factors as $(x - \eta)(x - \eta^2)$, so $\mathbb{Q}(\eta)/\mathbb{Q}$ is Galois (being the splitting field of a separable polynomial) and $\mathrm{Aut}(\mathbb{Q}(\eta)|\mathbb{Q})$ acts by permuting the roots η, η^2 of f_η.

The claim in (4) of the theorem is that the map

$$\mathrm{Aut}(E|\mathbb{Q}) \to \mathrm{Aut}(\mathbb{Q}(\eta)|\mathbb{Q})$$

given by restricting automorphisms of E to the subfield $\mathbb{Q}(\eta)$ induces an isomorphism $\mathrm{Aut}(E|\mathbb{Q})/H \simeq \mathrm{Aut}(\mathbb{Q}(\eta)|\mathbb{Q})$. All elements of H act trivially on $\mathbb{Q}(\eta)$, so their restriction is the identity map. The nontrivial coset of H is represented by any of $\tau = (12), (23)$, or (13). For any of these the corresponding action on η is given by

$$\phi_\tau(\eta) = \frac{\phi_\tau(\eta\theta)}{\phi_\tau(\theta)} = \eta^{\tau(1)-\tau(3)} = \eta^{-1} = \eta^2 .$$

Now consider the non-normal subgroup $G = \langle(12)\rangle < S_3$. The fixed field of G is $E^G = \mathbb{Q}(\theta)$. As seen before, this extension is not Galois. Note that restricting automorphisms of $E/\mathbb{Q}$ to $\mathbb{Q}(\theta)$ does not give automorphisms of $\mathbb{Q}(\theta)/\mathbb{Q}$. For example $\phi_{(13)}(\theta) = \eta\theta$ so the restriction of $\phi_{(13)}$ is the isomorphism $\mathbb{Q}(\theta) \to \mathbb{Q}(\eta\theta)$ sending θ to $\eta\theta$. Note that $\mathbb{Q}(\eta\theta) = \phi_{(13)}(E^G)$ is the fixed field of the $(13)G(13) = \langle(23)\rangle$ as indicated in part (3) of the correspondence theorem.

5. Galois groups of cyclotomic extensions

Theorem 5.1. *Let η be a primitive n-th root of unity. Then $\mathbb{Q}(\eta)/\mathbb{Q}$ is Galois and the map $i \mapsto (\sigma_i : \eta \mapsto \eta^i)$ determines an isomorphism $\mathbb{Z}/n\mathbb{Z}^\times \simeq \mathrm{Aut}(\mathbb{Q}(\eta)|\mathbb{Q})$.*

Corollary 5.2. *For every finite abelian group G there is a Galois extension $E/\mathbb{Q}$ with $\mathrm{Aut}(E|\mathbb{Q}) \simeq G$.*

Remark 5.3. *The 'Kronecker-Weber' theorem says that every finite abelian extension (i.e., Galois extension with abelian Galois group) of $\mathbb{Q}$ is contained in a cyclotmic extension $\mathbb{Q}(\eta_n)$ for some n.*

Example 5.4. *Analyze the extension $\mathbb{Q}(\eta)/\mathbb{Q}$ where η is a primitive 7-th root of unity.*

6. Finite Fields

Theorem 6.1. *Every finite field has order p^n for some prime p and integer n and for every prime power $q = p^n$ there is a (unique up to isomorphism) field $\mathbb{F}_q$ of order $q = p^n$; it is the splitting field over $\mathbb{F}_p$ of the polynomial $x^q - x$.*

Proof. First we claim that for any $q = p^n$ there is a field $\mathbb{F}_q$ of order q. Let E be the splitting field of $f = x^q - x$ over $\mathbb{F}_p$. The roots of f are distinct (since $\gcd(f, f') = \gcd(f, -1) = 1$) and so E has at least q elements. On the other hand, the roots of f form a subfield of E containing $\mathbb{F}_p$ (use that $(\alpha + \beta)^q = \alpha^q + \beta^q$). Hence E has order q.

Now suppose E is any finite field. Let F be the subfield generated by 1_E. SInce E is finite, $m \cdot 1_E = 0$ for some m and then $F \simeq \mathbb{Z}/m\mathbb{Z}$. But then m must be prime (otherwise F is not a field) and $q = p^n$ since E is a vector space over F. The polynomial $f = x^q - x = x(x^{q-1} - 1) \in \mathbb{F}_p[x]$ plits over E by Lagrange's theorem since $\#E^\times = q - 1$. Thus f splits over E and as every element of E is a root, E must be the splitting field. Since splitting fields are unique up to isomorphism, $E = \mathbb{F}_{p^n}$. □

Theorem 6.2. *For any p, n, the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois and $\mathrm{Aut}(\mathbb{F}_{p^n}|\mathbb{F}_p)$ is cyclic of order n, generated by the Frobenius map $F : \alpha \mapsto \alpha^p$.*

Proof. Check that F is an automorphism of $\mathbb{F}_{p^n}$ leaving $\mathbb{F}_p$ fixed and that F has order n. □

Corollary 6.3. *$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ if and only if $m \mid n$, in which case this subfield is unique.*

Proof. $\mathrm{Aut}(\mathbb{F}_{p^n}|\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$ has a (necessarily unique) subgroup H of order d if and only if $d \mid n$. The fixed field $(\mathbb{F}_{p^n})^H$ has size n/d. □

Example 6.4. *$\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$, where $\alpha^4 + \alpha + 1 = 0$. Compute the orbits and stabilizers of the elements of $\mathbb{F}_{16}$ under the action of $\mathrm{Aut}(\mathbb{F}_{16}|\mathbb{F}_2)$ and use this to find the factorization of $x^{16} - x$.*

7. Galois groups of low degree polynomials

In this section we assume for simplicity that F has characteristic 0. Let $f \in F[x]$ be a separable polynomial of degree n with splitting field E/F. As we have the action of $\mathrm{Gal}(f) = \mathrm{Aut}(E|F)$ on the roots $\theta_1, \ldots, \theta_n \in E$ of f allow us to identify $\mathrm{Gal}(f)$ with a subgroup of the symmetric group $\mathrm{Sym}\{\theta_1, \ldots, \theta_n\} \simeq S_n$. Moreover, the action of $\mathrm{Aut}(E|F)$ on E can be recovered from this. In this section we consider how to determine this subgroup for low degree polynomials (and describe an approach that can in principle work in general).

Definition 7.1.
The different of f is $\Delta(f) = \prod_{i<j}(\theta_i - \theta_j)$.
The discriminant of f is $D(f) = \Delta(f)^2$.

Remark 7.2. *The different depends up to ± 1 on the order of the roots $\theta_1, \ldots, \theta_n$. The discriminant does not depend on the choice of ordering.*

Example 7.3. Degree 2**:** *Let $f = x^2 + bx + c \in F[x]$. By the quadratic formula the roots of f are $\frac{-b \pm \sqrt{b^2-4c}}{2}$. So*

$$\Delta(f) = \sqrt{b^2 - 4c} \qquad D(f) = b^2 - 4c\,.$$

The Galois group of f is determined by whether or not the discriminant $D(f)$ is a square:

$$\mathrm{Gal}(f) = \begin{cases} S_2 & \text{if } (b^2 - 4c) \notin F^2 \\ 1 & \text{if } (b^2 - 4c) \in F^2 \end{cases}$$

Proposition 7.4. *$\mathrm{Gal}(f) < A_n$ if and only if $D(f) \in F^2$.*

This says that that the stabiliser of $\Delta(f)$ under $\mathrm{Gal}(f) \circlearrowright E$ is $\mathrm{Gal}(f) \cap A_n$.

Proof. For any $\sigma \in \mathrm{Gal}(f)$ we have $\sigma(\Delta(f)) = \mathrm{sgn}(\sigma)\Delta(f)$. So $\Delta(f) \in E^{\mathrm{Gal}(f)} = F$ if and only if $\mathrm{sgn}(\sigma) = 1$ for all $\sigma \in \mathrm{Gal}(f)$. □

7.1. **Degree** 3**.** Assume $f = x^3 + px + q \in F[x]$ is an irreducible degree 3 polynomial (all polynomials of degree 3 can be brought into this form by a change of variables to eliminate the x^2 term). Then $D(f) = -4p^3 - 27q^2$.

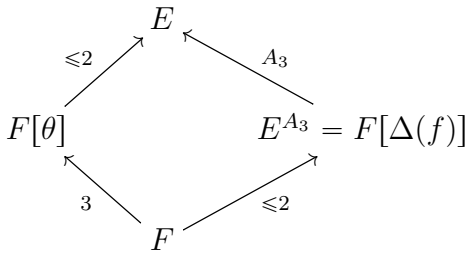
The Galois group of f is a transitive subgroup of S_3. The only transitive subgroups of S_3 are S_3 and A_3. Hence

$$\mathrm{Gal}(f) = \begin{cases} S_3 & \text{if } D(f) \notin F^2 \\ A_3 & \text{if } D(f) \in F^2 \end{cases}$$

TABLE 1. Transitive subgroups of S_4

	S_4	A_4	V	D_4	C_4
$[G \cap V : 1]$	4	4	4	4	2
$[G : G \cap V]$	6	3	1	2	2

To construct the splitting field we first adjoin a root θ of f to F. Then $F[\theta]$ is the splitting field (in which case the Galois group is order 3) or f factors as $(x-\theta)$ times an irreducible quadratic over $F[\theta]$ in which case the splitting field has degree 6.



For example, when $f = x^3 - 2$, we have $D(f) = -27 \times 2^2 = -2^2 \times 3^3 \notin \mathbb{Q}^2$. We also know that the quadratic intermediate field $\mathbb{Q} \subset M \subset E$ is $M = \mathbb{Q}(\eta)$, where η is a cube root of unity. Since $\eta = \frac{-1 \pm \sqrt{-3}}{2}$, we see $\mathbb{Q}(\eta) = \mathbb{Q}(\sqrt{D(f)})$ as expected.

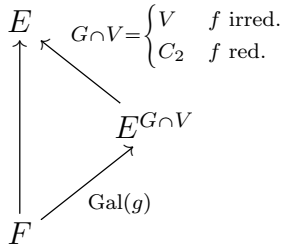
7.2. **Degree** 4**.** Suppose $f = x^4 + bx^3 + cx^2 + dx + e \in F[x]$ is an irreducible polynomial of degree 4. Computation of $G = \mathrm{Gal}(f)$ can be reduced to the computation of the Galois group of a cubic polynomial called the resolvent cubic. This is the polynomial

$$g = x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 = (x-\alpha)(x-\beta)(x-\gamma)\,,$$

where

$$\begin{aligned} \alpha &= \theta_1\theta_2 + \theta_3\theta_4 \\ \beta &= \theta_1\theta_3 + \theta_2\theta_4 \\ \gamma &= \theta_1\theta_4 + \theta_2\theta_3\,. \end{aligned}$$

Note that each of α, β, γ is fixed by V. In fact, one can show that $E^{G\cap V} = F[\alpha, \beta, \gamma]$ is the splitting field of the resolvent cubic. Therefore $[G : G \cap V] = G/(G \cap V) = \mathrm{Gal}(g)$, where g is the resolvent cubic. Having computed this, we determine G using Table 1. This works except in the case where $[G : G \cap V] = 2$. Then one must also consider $[G \cap V : 1]$, which is determined by whether or not f is irreducible over $E^{G\cap V}$.



Example 7.5. *$f = x^4 - 4x + 2 \in \mathbb{Q}[x]$ is irreducible by Eisenstein's criterion with $p = 2$. The cubic resolvent is $g = x^3 - 8x + 16$ which has discriminant -4864. This not a square, so $E^{G\cap V}$ is an S_3 extension of $\mathbb{Q}$. From the table we see* $\mathrm{Gal}(f) = S_4$.

Example 7.6. *$f = x^4 + 4x^2 + 2 \in \mathbb{Q}[x]$ is irreducible and has cubic resolvent $(x-4)(x^2-8)$, so $E^{G\cap V} = \mathbb{Q}(\sqrt{2})$ and $[G : G \cap V] = 2$. To determine the $G = \mathrm{Gal}(f)$ we check if f is irreducible over $\mathbb{Q}(\sqrt{2})$. It is not (use the quadratic formula on f as a polynomial in x^2), so* $\mathrm{Gal}(f) = C_4$.

8. The Fundamental Theorem of Algebra

The complex numbers are constructed by adjoining a square root of -1 to $\mathbb{R}$. Namely, let $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}[x]/\langle x^2 + 1\rangle$. In this seciton we show how one can use Galois theory to give a proof of the following theorem.

Theorem 8.1. *Every nonconstant polynomial $f \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.*

This means that there are no algebraic extensions of the field $\mathbb{C}$. A field with this property is said to be algebraically closed.

The proof will use the following four results:

(1) There are no extensions of $\mathbb{R}$ of odd degree > 1;
(2) There are no extensions of $\mathbb{C}$ of degree 2;
(3) Sylow-2-subgroups exist;
(4) 2-groups are solvable.

The first two are results in analysis which follow from the Intermediate Value Theorem. The second two are results in group theory which we have proved in earlier sections. Galois theory will be used to conclude the theorem from this results by relating groups to field extensions.

Let us prove (1): the existence of an odd degree extension is equivalent to the existence of an irreducible polynomial of odd degree $f \in \mathbb{R}[x]$. But if f has odd degree $\lim_{x\to\infty} f(x) = -\lim_{x\to-\infty} f(x)$, so $f(x) = 0$ has a solution by IVT. Thus f has a root and is therefore not irreducible.

Let us prove (2): First note that IVT implies that all nonnegative reals have a real square root (apply IVT to $f = x^2 - a$). Now if $z = a + bi$, then $z = (c + di)^2$ where $c^2 = \frac{a+\sqrt{a^2+b^2}}{2}$, $d^2 = \frac{-a+\sqrt{a^2+b^2}}{2}$.

Lemma 8.2. *The theorem holds if and only if every nonconstant polynomial $f \in \mathbb{R}[x]$ has a root in $\mathbb{C}$.*

Proof. Given $g \in \mathbb{C}[x]$ we can write $g = a + ib$ with $a, b \in \mathbb{R}[x]$. Then $h = (a + bi)(a - bi) = a^2 + b^2 \in \mathbb{R}[x]$ has a root if and only if g has a root. □

Proof of Theorem 8.1. Let $f(x) \in \mathbb{R}[x]$ and let E be the splitting field of $(x^2 + 1)f(x)$ over $\mathbb{R}$. Let $G = \mathrm{Gal}(E/\mathbb{R})$ and let $H < G$ be a Sylow-2-subgroup. Then $[E^H : \mathbb{R}] = [G : H]$ is odd. It follows that $E^H = \mathbb{R}$, since $\mathbb{R}$ has no proper odd degree extensions. Then $H = \mathrm{Aut}(E|E^H) = \mathrm{Aut}(E|\mathbb{R}) = G$, so G is a 2-group. Since $\mathbb{R} \subset \mathbb{C} \subset E$ is an intermediate

field we have $\mathrm{Aut}(E|\mathbb{C}) < E$ is a subgroup of index 2. Then $\mathrm{Aut}(E|\mathbb{C})$ is also a 2-group, hence solvable. Therefore we can find a chain of normal subgroups

$$\mathrm{Gal}(E|\mathbb{C}) \rhd G_1 \rhd \cdots \rhd G_n = 1\,,$$

such that the subsequent quotients are all isomorphic to $\mathbb{Z}_2$.

Corresponding to these subgroups we have a chain of fields

$$\mathbb{C} = E^{\mathrm{Gal}(E|\mathbb{C})} \subset E^{G_1} \subset \cdots \subset E^{G_n} = E\,,$$

where each is an extension of degree 2 of the previous. However, there are no extensions of $\mathbb{C}$ of degree 2, so in fact this chain must have length 1. This means $E = \mathbb{C}$. So all of the roots of f are contained in $\mathbb{C}$. □

9. Constructible Numbers

A real number α is said to be constructible if given a line segment of unit length, a line segment of length $|\alpha|$ can be constructed using a straightedge and compass in a finite number of steps. A point in the Euclidean plane is constructible if it is either the end point of a constructed segment or the intersection of two constructed lines. A classical (i.e., going back at least to ancient Greek mathematicians such as Plato) problem is to construct a regular n-gon. Gauss claimed the following characterization of constructible numbers in 1801, though the first rigorours proof was given by Lindemann 1882. This allows one to determine exactly which n-gons can be constructed.

Theorem 9.1. *A real number $\alpha \in \mathbb{R}$ is constructible if there is a tower of field extensions*

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots F_n$$

with $[F_m : F_{m-1}] = 2$ for each $m = 1, \ldots, n$ and $\alpha \in F_n$.

Corollary 9.2 (Gauss)**.** *Let p be a prime. The regular p-gon is constructible if and only if $p = 2^n + 1$ for some n.*

Proof. The regular n-gon is constructible if and only if the cosine of the interior angle $\cos(2\pi/n)$ is a constructible number. Let $\eta = e^{2\pi i/p}$ be a primitive p-th root of unity. Then $\cos(2\pi/p) = (\eta + \overline{\eta})/2 \in \mathbb{R}$. This generates the maximal totally real subfield of the cyclotomic extension $\mathbb{Q}(\eta)$, which has Galois group $(\mathbb{Z}/p\mathbb{Z})^\times \simeq C_{p-1}$. Hence $\mathbb{Q}(\cos(2\pi/p))/\mathbb{Q}$ is Galois with Galois group $C_{(p-1)/2}$. Therefore there is exactly one intermediate field $\mathbb{Q} \subset M \subset \mathbb{Q}(\cos(2\pi/p))$ for each divisor d of $(p-1)/2$. So $\mathbb{Q}(\cos(2\pi/p))$ sits at the top of a tower of quadratic extensions if and only if $(p-1)/2 = 2^k$. □

Remark 9.3. *Primes of the form $p = 2^n + 1$ are called Fermat Primes. It is not known whether or not there are infinitely many Fermat primes. It is known that any Fermat prime is actually of the form $2^{2^n}+1$. The only ones that are known are $3 = 2^{2^0}$, $5 = 2^{2^1}$, $17 = 2^{2^2}+1$, $257 = 2^{2^3}+1$, $65537 = 2^{2^4}+1$. But $2^{2^5}+1 = 4294967297 = 641 \times 6700417$ is not prime.*

10. The Abel-Rufini Theorem

Definition 10.1. *An extension E/F is called radical if there are intermediate fields*

$$F_0 = F \subset F_1 \subset \cdots \subset F_i = E\,,$$

integers $n_i \geqslant 2$ and $\alpha_i \in F_{i-1}$ such that $F_i = \frac{F_{i-1}[x]}{\langle x^{n_i} - \alpha_i \rangle}$.

A polynomial $f \in F[x]$ is said to be solvable if it splits in a some radical extension.

In other words, every extension in this tower is obtained by adjoining an n-th root of an element from the previous extension. Note that any element $\alpha \in E$ a radical extension of F has an algebraic expression . A polynomial is solvable if and only if there is an algebraic expression of its roots involving only elements of F, basic arithmetic symbols $+, -, \times, \div$ and radicals $\sqrt[n]{}$.

Example 10.2. *$f = x^4 - 4x^2 + 2$ is solvable since its roots are given by*

$$\pm\sqrt{\frac{2 \pm \sqrt{2}}{2}}$$

Example 10.3. *If η is a primitive 17-th root of unity then $\alpha = 2\cos(2\pi/p) = (\eta + \overline{\eta})$ lives in the Galois extension $\mathbb{Q}(\eta)/\mathbb{Q}$. SInce the Galois group is a 2-group this extension is radical. The minimal polynomial of α is*

$$f := x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 + 10x^3 - 10x^2 - 4x + 1\,.$$

In fact

$$16\,\cos\frac{2\pi}{17} = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{170 + 38\sqrt{17}.}}\cdot$$

Example 10.4. *Let $F = \mathbb{Q}(a, b)$, where a, b are indeterminates (i.e., trancendental over $\mathbb{Q}$). The 'general quadratic polynomial' is $f = x^2 + ax + b \in \mathbb{Q}(a, b)[x]$. By the quadratic formula, f splits in the radical extension $F \subset F(\sqrt{a^2 - 4b}) = \mathbb{Q}(a, b)[\sqrt{a^2 - 4b}]$. The cubic and quartic formulas show similarly that the general cubic and quartic polynomials are also solvable. Consequently all polynomials $f \in \mathbb{Q}[x]$ of degree $\leqslant 4$ are solvable.*

Theorem 10.5 (Abel-Rufini Theorem)**.** *The general quintic polynomial is not solvable in radicals. This means that the splitting field of*

$$x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Q}(a_0, \ldots, a_4)$$

is not contained in any radical extension of $\mathbb{Q}(a_0, \ldots, a_4)$.

Thus there is no 'quintic formula' analgous to the quadratic formula. Abel-Rufini does not rule out the possibility of solving some quintic polynomials in radicals (and in fact polynomials like $x^5 - 2$ can obviously be solved in radicals), nor does it rule out the possibility that every $f \in \mathbb{Q}[x]$ is solvable; a priori it could be that for every polynomial $f \in \mathbb{Q}[x]$ there is a radical expression for its roots. The theorem only says that there is no one quintic formula which works for them all. Galois went further and used the theory he developed to characterise when polynomials are solvable in terms of their Galois group. Using this he showed that there are indeed quintic polynomials over $\mathbb{Q}$ that are not solvable.

Theorem 10.6 (Galois)**.** *Let F be a field of characteristic zero. A polynomial $f \in F[x]$ is solvable if and only if its Galois group is solvable.*

This is the reason why solvable groups are called solvable. Recall that this means that all of the Jordan-Hölder factors are cyclic groups. The connection between this and radical extensions is given by the following lemma.

Lemma 10.7. *Suppose F contains a primitive n-th root of unity. Then $F[\sqrt[n]{a}]/F$ is Galois with cyclic Galois group for any $a \in F$.*

Proof. Exercise. □

Proof of Theorem 10.6. We prove one direction. Suppose $f \in F[x]$ is solvable in radicals and let E be the splitting field of f over F. So we have fields $F_i = F_{i-1}[\alpha_i]$, $\alpha_i^{n_i} = a_i \in F_{i-1}$ such that $E \subset F_m$. Let n be the least common multiple of the n_i. Let Ω be a Galois extension of F containing F_m and a primitive n-th root of unity (for example, take generators $\gamma_1, \ldots, \gamma_k$ for F_m/F and let Ω be the splittinf field of the product of the minimal polynomials of the γ_i and $x^n - 1$).

Let $g = (x^n - 1)\prod_{i=1}^m \prod_{\sigma \in \mathrm{Gal}(\Omega|F)}(x^{n_i} - \sigma(a_i)) \in F[x]$ and let E' be the splitting field of g over F. Then E'/F is Galois, E' contains $F_m[\eta]$ and hence E. Also E' sits in a tower of fields

$$F \subset E_1 = F[\eta] \subset E_2 = E_1[\alpha_1] \subset \cdots \subset E_\ell = E'$$

where each extension (after the first) is obtained by adjoining an n-th root of some element. In particular each step has abelian Galois group, so the Galois group of E'/F is solvable.

The splitting field E of f is an intermediate field $F \subset E \subset E'$, so $\mathrm{Gal}(E|F)$ is a quotient of $\mathrm{Gal}(E'|F)$. A quotient of a solvable group is solvabe, so $\mathrm{Gal}(E|F)$ is solvable. □

Before proving the converse, we need a lemma:

Lemma 10.8. *Let F be a field and $\sigma_1, \ldots, \sigma_n$ distinct automorphisms of F. Suppose that $a_1, \ldots, a_n$ are elements of F such that $\sum a_i\sigma_i(x) = 0$ for all $x \in F$. Then $a_1 = \cdots = a_n = 0$.*

Proof. Induction on n. For $n = 1$, $a_1 = a_1\sigma_1(1) = 0$. For $n > 1$, if $\sum a_i\sigma_i(x) = 0, x \in F$ and $a \in F$ then $0 = \sum a_i\sigma_i(ax) = \sum a_i\sigma_i(x)\sigma_i(a)$. On the other hand $\sum a_i\sigma_i(x)\sigma_1(a) = 0$. Subtracting the last two equations gives $\sum a_i\sigma_i(x)(\sigma_i(a) - \sigma_1(a)) = 0$. This equation has $n - 1$ terms so, by the induction hypothesis, either $a_i = 0$, for all $i > 1$ or $\sigma_i(a) - \sigma_1(a) = 0$ for some $i > 1$. In the first case we also get $a_1 = 0$ and we are done. In the second case, since a was arbitrary, we get $\sigma_1 = \sigma_i$, contrary to the hypothesis, and we are also done. □

Proof of converse direction of Theorem 10.6. Since $\mathrm{Gal}(f)$ is solvable, it has a composition series consisting of cyclic groups of prime order, which translates into the splitting field E of f over F being the top of a tower of extensions all of which are cyclic of prime orders. The following lemma then gives the result:

Lemma 10.9. *Let L/K be a cyclic extension of prime degree $p \neq \mathrm{char}K$ with Galois group generated by σ and assume that K contains a primitive p-th root of unity ζ. Then there exists $a \in K$ such that L is the splitting field of $x^p - a \in K[x]$.*

Proof. The above lemma allows us to find $x \in F$ such that $u = \sum_{j=0}^{p-1} \zeta^j\sigma^j(x) \neq 0$. We have that $\sigma(u) = \zeta^{-1}u \neq u$ so $u \notin K$ and therefore $L = K(u)$, since $[L : K]$ is prime. But the same equation also implies that $\sigma(u^p) = u^p$ so $a = u^p \in K$. It follows that L is the splitting field of $x^p - a \in K[x]$. □

□

To conclude that there are indeed polynomials over $\mathbb{Q}$ that are not solvable it suffices to prove the following lemma.

Lemma 10.10. *For any prime p there is an irreducible polynomial $f \in \mathbb{Q}[x]$ whose Galois group is S_p, which is not solvable.*

Proof. Suppose $f \in \mathbb{Q}[x]$ is irreducible of degree p and has exactly $p-2$ real roots. Then complex conjugation gives an element of order 2 in the Galois group of f. On the other hand $p \mid \#\operatorname{Gal}(f)$, so $\operatorname{Gal}(f)$ contains an element of order p by Cauchy's theorem. Now use that S_p is generated by any transposition and any p-cycle. □

We can also use Galois' theorem to derive the Abel-Rufini theorem:

Let $r_1, \ldots, r_n$ be indeterminates and consider the field $E = \mathbb{Q}(r_1, \ldots, r_n)$. There is an obvious action of S_n on E by field automorphisms which permutes the r_i according to $\sigma(r_i) = r_{\sigma(i)}$. Let $F = E^{S_n}$ be the fixed field of this action. Then E/F is Galois with Galois group S_n. Moreover, $F = \mathbb{Q}(p_1, \ldots, p_n)$ where the p_i are the symmetric polynomials in the r_i, i.e.

$$\begin{aligned} p_1 &= r_1 + r_2 + \cdots + r_n \\ p_2 &= \sum i < j r_i r_j \\ &\vdots \\ p_{n-1} &= \sum_{i_1 < \cdots < i_{n-1}} r_{i_1} \cdots r_{i_{n-1}} \\ p_n &= r_1 r_2 \cdots r_n \end{aligned}$$

If a_i are indeterminates then $\mathbb{Q}(a_1, \ldots, a_n) \to \mathbb{Q}(p_1, \ldots, p_n)$ sending a_i to p_i is an isomorphism[1] and it follows that the Galois group of the generic polynomial of degree n is S_n.

Lemma 10.9 does not describe the degree p cyclic extensions in characteristic p. This case is covered by the following result.

Lemma 10.11. *Let L/K be a cyclic extension of prime degree $p = \operatorname{char} K$ with Galois group generated by σ. Then there exists $a \in K$ such that L is the splitting field of $x^p - x - a \in K[x]$. Conversely, the polynomial $x^p - x - a \in K[x]$ either splits in K or is irreducible, with Galois group cyclic of order p.*

Proof. If α is a root of $x^p - x - a$, then so is $\alpha + 1$, hence the roots are $\alpha + j, j \in \mathbb{F}_p$ and $x^p - x - a$ is separable. If $g(x)$ is an irreducible factor of $x^p - x - a$, σ an automorphism of the splitting field E of $g(x)$ over K, and α a root of $x^p - x - a$ in E, then $\sigma(\alpha) = \alpha + j, j \in \mathbb{F}_p$. If $j \neq 0$, then all roots of $x^p - x - a$ are roots of $g(x)$ and $x^p - x - a$ is irreducible. If $j = 0$ for every choice of σ, then $g(x)$ has degree one and $x^p - x - a$ splits in K. So $x^p - x - a \in K[x]$ either splits in K or is irreducible, with Galois group cyclic of order p.

Conversely, if L/K is a cyclic extension of prime degree $p = \operatorname{char} K$ with Galois group generated by σ, choose $\beta \in L$ with $\operatorname{Tr}(\beta) := \beta + \sigma(\beta) + \cdots + \sigma^{p-1}(\beta) \neq 0$, which is possible by Lemma 10.8. Now, define

$$\alpha := (\beta + 2\sigma(\beta) + \cdots + p\sigma^{p-1}(\beta))/\operatorname{Tr}(\beta).$$

It follows immediately that $\sigma(\alpha) = \alpha - 1$, so $a := \alpha^p - \alpha \in K$, since it is invariant under σ and α is a root of $x^p - x - a$ in L but not in K so $L = K(\alpha)$, completing the proof. □

[1] This requires proof