# Galois Theory and Solvability



This copy of the text was compiled from source at 16:43 on 2/2/2023.

We will be glad to receive corrections and suggestions for improvement at guichard@whitman.edu.

# Contents

# 1

# Galois Theory

## 1.1 The Galois Group

We assume throughout that all fields have characteristic 0, unless otherwise indicated. References to Gallian are to the seventh edition.

**DEFINITION 1.1.1** If $E \supseteq F$ are fields, The *Galois group* $G(E/F)$ is the group of automorphisms of $E$ that fix every element of $F$. □

**DEFINITION 1.1.2** If $H \leq G(E/F)$, then $E_H$ is the fixed field of $H$, namely, the set of elements of $E$ that are fixed by every automorphism in $H$. □

**THEOREM 1.1.3** Suppose that $\sigma_1, \ldots, \sigma_n$ are distinct automorphisms of $E$. If $a_1$, $a_2$, $\ldots$, $a_n$ are elements of $E$ and for all $u \in E$

$$a_1\sigma_1(u) + \cdots + a_n\sigma_n(u) = 0,$$

then $a_i = 0$ for all $i$. In other words, no nontrivial linear combination of the functions $\sigma_i$ is the identically zero function.

***Proof.*** The contrapostive of the theorem is: Given that $\sigma_1, \ldots, \sigma_n$ are distinct automorphisms of $E$: If $a_1$, $a_2$, $\ldots$, $a_n$ are not all zero then there is a $u \in E$ such that

$$a_1\sigma_1(u) + \cdots + a_n\sigma_n(u) \neq 0.$$

To prove this it suffices to show that for all $m$, with $\sigma_1, \ldots, \sigma_m$ distinct automorphisms, if $a_1, \ldots, a_m$ are all nonzero, then there is a $u \in E$ such that

$$a_1\sigma_1(u) + \cdots + a_m\sigma_m(u) \neq 0.$$

This is because given $a_1$, $a_2$, ..., $a_n$ not all zero, we may pick out the $m$ of them that are non-zero, and apply the second result.

So we prove the following statement by induction on $m$: If $\sigma_1, \ldots, \sigma_m$ are any distinct automorphisms of $E$, and $a_1, \ldots, a_m$ are all nonzero then for some $u$, $a_1\sigma_1(u) + \cdots + a_m\sigma_m(u) \neq 0$. Call this statement "$S(m)$."

Base: If $m = 1$, pick $u$ so that $\sigma_1(u) \neq 0$ ($u = 1$, for example). Then $a_1\sigma_1(u) \neq 0$ because $E$ has no zero divisors.

Induction: We want to prove that if $S(i)$ is true for $i \leq m$, then $S(m+1)$ is true. We prove the contrapositive, namely, that if $S(m+1)$ is false, then $S(i)$ is false for some $i \leq m$. So suppose that $a_1, \ldots, a_{m+1}$ are nonzero and for all $u$, $a_1\sigma_1(u) + \cdots + a_{m+1}\sigma_{m+1}(u) = 0$. Pick $a \in E$ such that $\sigma_1(a) \neq \sigma_{m+1}(a)$. Now substituting $au$ for $u$ and then using the multiplication-preserving property of isomorphisms we get:

$$\begin{aligned} 0 &= a_1\sigma_1(au) + \cdots + a_m\sigma_m(au) + a_{m+1}\sigma_{m+1}(au) \\ 0 &= a_1\sigma_1(a)\sigma_1(u) + \cdots + a_m\sigma_m(a)\sigma_m(u) + a_{m+1}\sigma_{m+1}(a)\sigma_{m+1}(u). \end{aligned} \tag{1.1.1}$$

Also,

$$\begin{aligned} 0 &= \sigma_{m+1}(a)\big(a_1\sigma_1(u) + \cdots + a_m\sigma_m(u) + a_{m+1}\sigma_{m+1}(u)\big) \\ 0 &= a_1\sigma_{m+1}(a)\sigma_1(u) + \cdots + a_m\sigma_{m+1}(a)\sigma_m(u) + a_{m+1}\sigma_{m+1}(a)\sigma_{m+1}(u). \end{aligned} \tag{1.1.2}$$

Subtracting equation 1.1.2 from equation 1.1.1, we get

$$0 = a_1(\sigma_1(a) - \sigma_{m+1}(a))\sigma_1(u) + \cdots + a_m(\sigma_m(a) - \sigma_{m+1}(a))\sigma_m(u).$$

Not all of the coefficients of the $\sigma_i$ are zero in the last equation, because $a_1(\sigma_1(a) - \sigma_{m+1}(a)) \neq 0$. Choosing just those terms in which $a_j(\sigma_j(a) - \sigma_{m+1}(a)) \neq 0$, we have shown that for some $i \leq m$, $S(i)$ is false, as desired. ∎

**THEOREM 1.1.4** If $[E:F] < \infty$, then $G(E/F)$ is finite and in fact $|G(E/F)| \leq [E:F]$.

***Proof.*** Let $u_1, \ldots, u_n$ be a basis for $E$ over $F$. Suppose, for a contradiction, that $G(E/F)$ contains $n+1$ distinct automorphisms, $\sigma_1, \ldots, \sigma_{n+1}$. Consider the system of $n$ simultaneous equations in $n+1$ unknowns:

$$\sum_{i=1}^{n+1} \sigma_i(u_j)x_i = 0, \qquad j = 1 \ldots n. \tag{1.1.3}$$

By linear algebra, this system has a nontrivial solution $a_1, \ldots, a_{n+1}$. Now for any $u \in E$, $u = \sum_{i=1}^{n} c_i u_i$, because the $u_i$ form a basis. Then

$$\sum_{i=1}^{n+1} a_i\sigma_i(u) = \sum_{i=1}^{n+1} a_i \sum_{j=1}^{n} c_j\sigma_i(u_j) = \sum_{j=1}^{n} c_j \sum_{i=1}^{n+1} a_i\sigma_i(u_j) = \sum_{j=1}^{n} c_j \cdot 0 = 0,$$

because $a_1, \ldots, a_{n+1}$ is a solution to the system of equations in 1.1.3. This contradicts theorem 1.1.3. ■

## 1.2 Symmetric functions

**DEFINITION 1.2.1** The elementary symmetric functions in $\{x_1, \ldots, x_n\}$ are

$$a_j = \sum_{X \in \binom{[n]}{j}} \prod_{i \in X} x_i,$$

where $\binom{[n]}{j}$ is the collection of all subsets of $\{1, 2, \ldots, n\}$ of size $j$. In other words, $a_j$ is the sum of all possible terms formed by multiplying $j$ of the $x_i$ together. □

*Remark.* The elementary symmetric functions arise quite naturally:

$$\prod_{i=1}^{n} (t - x_i) = t^n - a_1 t^{n-1} + a_2 t^{n-2} - \cdots + (-1)^n a_n$$

is a polynomial with roots $x_i$.

**LEMMA 1.2.2** If $E$ is the splitting field for $f(x)$ over $F$, then $[E : F] \leq n!$, where $n$ is the degree of $f$.

***Proof.*** By induction on $n$. Let $b$ be a root of $f$ in $E$. Since $b$ is the root of a polynomial of degree $n$, $[F(b) : F] \leq n$. Also, $(x - b)$ must divide $f(x)$ over $F(b)$, so let $g(x) = f(x)/(x - b)$. $E$ is the splitting field for $g(x)$ over $F(b)$, so by the induction hypothesis, $[E : F(b)] \leq (n - 1)!$. Now

$$[E : F] = [E : F(b)][F(b) : F] \leq n(n - 1)! = n!.$$

■

**THEOREM 1.2.3** If $F$ is a field, $F(\bar{x})$ is the field of rational functions in the variables $\bar{x} = \{x_1, \ldots, x_n\}$. Let $S \subseteq F(\bar{x})$ be the subfield fixed by the symmetric group $S_n$, interpreted as acting on $\{x_1, \ldots, x_n\}$. Then

**a.** $[F(\bar{x}) : S] = n!$

**b.** $G(F(\bar{x})/S) = S_n$

**c.** $S = F(\bar{a})$

**d.** $F(\bar{x})$ is the splitting field of some polynomial over $S$

***Proof.*** The elementary symmetric functions $a_i$ are clearly in $S$, so $F(a_1, \ldots, a_n) \subseteq S$. The polynomial $p(t) = \prod_{i=1}^{n}(t - x_i)$ splits in $F(\bar{x})$ and has coefficients in $F(\bar{a})$, and in fact $F(\bar{x})$ is the splitting field of $p(t)$, since $F(\bar{x})$ is the smallest field containing all of the roots $x_i$. By the lemma,

$$[F(\bar{x}) : F(\bar{a})] \leq n!. \tag{1.2.1}$$

Thus, $[F(\bar{x}) : S]$ is finite, and since $S_n \leq G(F(\bar{x})/S)$,

$$[F(\bar{x}) : S] \geq |G(F(\bar{x})/S)| \geq |S_n| = n!. \tag{1.2.2}$$

Combining equations 1.2.2 and 1.2.1,

$$n! \geq [F(\bar{x}) : F(\bar{a})] = [F(\bar{x}) : S][S : F(\bar{a})] \geq n![S : F(\bar{a})] \geq n!.$$

Thus $[S : F(\bar{a})] = 1$ so $S = F(\bar{a})$, and $[F(\bar{x}) : S] = n!$. Now using equation 1.2.2 again, $|G(F(\bar{x})/S)| = n!$, and so $G(F(\bar{x})/S) = S_n$. ∎

## 1.3 Normal extensions

**DEFINITION 1.3.1** $E$ is a normal extension of $F$ if $[E : F] < \infty$ and $F = E_{G(E/F)}$. □

**THEOREM 1.3.2** If $[E : F] < \infty$ and $H \leq G(E/F)$, then

**a.** $[E : E_H] = |H|$

**b.** $H = G(E/E_H)$

If $E$ is a normal extension of $F$, $[E : F] = |G(E/F)|$.

***Proof.*** Since $H$ fixes $E_H$, $H \leq G(E/E_H)$. By theorem 1.1.4, $[E : E_H] \geq |G(E/E_H)| \geq |H|$. If we can show that $|H| \geq [E : E_H]$ then both (a) and (b) follow immediately.

Since $[E : E_H] < \infty$, $E = E_H(a)$ for some $a$, by the Primitive Element Theorem. Let $q(t)$ be the minimal polynomial of $a$ over $E_H$, with degree $m = [E : E_H]$. Recall that by the Divisibility Property (Gallian theorem 20.3), $q(t)$ divides any polynomial over $E_H$ that has $a$ as a root.

Let $H = \{\epsilon = \sigma_1, \sigma_2, \ldots, \sigma_h\}$, where $\epsilon$ is the identity automorphism. We want to prove that $h \geq m$. Consider the elementary symmetric functions using $\sigma_i(a)$ in place of $x_i$:

$$\alpha_1 = \sum_{i=1}^{h} \sigma_i(a) \quad \alpha_2 = \sum_{i<j} \sigma_i(a)\sigma_j(a) \quad \ldots \quad \alpha_j = \sum_{X \in \binom{[h]}{j}} \prod_{i \in X} \sigma_i(a) \quad \ldots \quad \alpha_h = \prod_{i=1}^{h} \sigma_i(a)$$

For convenience, let $\alpha_0 = 1$. Now we note that

$$\sigma_k(\alpha_j) = \sum_{X \in \binom{[h]}{j}} \prod_{i \in X} (\sigma_k \circ \sigma_i)(a).$$

Since $H$ is a group, $\{\sigma_k \circ \sigma_i : i = 1, \ldots, h\}$ is simply a permutation of $\{\sigma_1, \sigma_2, \ldots, \sigma_h\}$, and since $\alpha_j$ is symmetric in the $\sigma_i$, $\sigma_k(\alpha_j) = \alpha_j$. Hence, for all $j$, $\alpha_j \in E_H$. Now let

$$p(t) = \prod_{i=1}^{h}(t - \sigma_i(a)) = \sum_{i=0}^{h}(-1)^i \alpha_i t^{h-i}.$$

Since $\sigma_1(a) = a$, $p(a) = 0$, and since $p(t) \in E_H[t]$, $q(t)$ divides $p(t)$. Since the degree of $q$ is $m$ and the degree of $p$ is $h$, $h \geq m$, as desired.

For the last statement of the theorem, let $H = G(E/F)$. Then by normality and parts (a) and (b), $[E : F] = [E : E_H] = |H| = |G(E/F)|$. ■

**LEMMA 1.3.3** Suppose $E$ is the splitting field for $f$ over $F$, and $p$ is an irreducible polynomial in $F[x]$ that divides $f$ over $F$. Let the roots of $p$ be $a_1, \ldots, a_r$. Then for all $i$ there is a $\sigma \in G(E/F)$ such that $\sigma(a_1) = a_i$.

***Proof.*** Since the $a_i$ are roots of $f$, all $a_i$ are in the splitting field $E$. By the lemma on page 372 in Gallian, there is an isomorphism $\phi$ from $F(a_1)$ to $F(a_i)$ that takes $a_1$ to $a_i$ and fixes $F$. $E$ is the splitting field for $f$ over both $F(a_1)$ and $F(a_i)$, so by theorem 19.4 in Gallian, there is an automorphism $\sigma$ on $E$ that extends $\phi$—this $\sigma$ is the desired automorphism, and the proof of the lemma is complete. ■

**THEOREM 1.3.4** $E$ is a normal extension of $F$ if and only if $E$ is the splitting field of some polynomial over $F$.

***Proof.*** Suppose $E$ is a normal extension of $F$. As in the previous proof, let $E = F(a)$, $G(E/F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, and

$$p(t) = \prod_{i=1}^{n}(t - \sigma_i(a)) = \sum_{i=0}^{n}(-1)^i \alpha_i t^{n-i},$$

where as before the $\alpha_i$ are the elementary symmetric functions in the $\sigma_i$. Since the $\alpha_i$ are fixed by $G(E/F)$, $\alpha_i \in F$ for every $i$. Thus, $p(t) \in F[t]$ and $p$ splits in $E$. Since $a$ is a root of $p$, $a$ must be in the splitting field of $p$, but since $E = F(a)$, this means $E$ is the splitting field of $p$.

Now, suppose $E$ is the splitting field for $f$ over $F$; we want to show that $E$ is a normal extension of $F$. The proof is by induction on $[E : F]$.

*Base* If $[E : F] = 1$, then $E = F$, $F$ is trivially the fixed field of $G(F/F)$ and so $E$ is a normal extension of $F$.

*Induction step* The inductive hypothesis is:

*If $E_1$ is an extension of $F_1$ with $[E_1 : F_1] < [E : F]$, and $E_1$ is a splitting field over $F_1$, then $E_1$ is a normal extension of $F_1$.*

Let $[E : F] = n > 1$. The polynomial $f$ has an irreducible factor $p$ of degree $r > 1$. By theorem 19.6 in Gallian, $p$ has distinct roots $a_1, \ldots, a_r$. Since $[E : F] = [E : F(a_1)][F(a_1) : F]$, $[E : F(a_1)] = [E : F]/[F(a_1) : F] = n/r < n$. Since $E$ is the splitting field of $f$ over $F(a_1)$, $E$ is a normal extension of $F(a_1)$, by the inductive hypothesis.

We need to show that the fixed field of $G(E/F)$ is $F$, that is, that if $a \in E$ is fixed by $G(E/F)$, then $a \in F$. Since $G(E/F(a_1)) \leq G(E/F)$, $a$ is fixed by $G(E/F(a_1))$ and so $a \in F(a_1)$ since $E$ is a normal extension of $F(a_1)$. By theorem 19.3 in Gallian,

$$a = c_0 + c_1 a_1 + c_2 a_1^2 + \cdots + c_{r-1} a_1^{r-1},$$

where the $c_i$ are in $F$. By lemma 1.3.3, for every $i$ there is a $\sigma_i \in G(E/F)$ such that $\sigma_i(a_1) = a_i$, so

$$\sigma_i(a) = a = c_0 + c_1 a_i + c_2 a_i^2 + \cdots + c_{r-1} a_i^{r-1}.$$

Thus, every $a_i$ is a root of the polynomial

$$(c_0 - a) + c_1 t + c_2 t^2 + \cdots + c_{r-1} t^{r-1}$$

of degree $r-1$. Since the $a_i$ are distinct, this implies that the coefficients of this polynomial are all 0, and in particular $a = c_0 \in F$.

■

## 1.4 Fundamental Theorem of Galois Theory

If $E \supseteq K \supseteq F$ and $E$ is a normal extension of $F$, then $E$ is a splitting field over $F$, so $E$ is a splitting field over $K$, and therefore $E$ is a normal extension of $K$. It need not be the case that $K$ is a normal extension of $F$. The next lemma characterizes those $K$ that are normal extensions of $F$.

**LEMMA 1.4.1** If $E \supseteq K \supseteq F$, and $E$ is a normal extension of $F$, then $K$ is a normal extension of $F$ if and only if for all $\sigma \in G(E/F)$, $\sigma(K) \subseteq K$.

***Proof.*** Suppose that for all $\sigma \in G(E/F)$, $\sigma(K) \subseteq K$. Let $K = F(a)$, then for all $\sigma \in G(E/F)$, $\sigma(a) \in K$. Let $p(x) = \prod_{\sigma \in G(E/F)} (x - \sigma(a))$. As in the proof of theorem 1.3.4, $p(x) \in F[x]$ and $K$ is the splitting field of $p(x)$ over $F$. Hence $K$ is a normal extension of $F$.

For the converse, suppose $K$ is a normal extension of $F$ and $K = F(a)$. Let $p(x) = \prod_{\sigma \in G(K/F)} (x - \sigma(a))$—note the $K$! Then just as in the proof of theorem 1.3.4, $K$ is the

splitting field of $p(x)$ over $F$, and $p(a) = 0$. Then for every $\sigma \in G(E/F)$ (note the $E$!), $0 = \sigma(p(a)) = p(\sigma(a))$, so $\sigma(a)$ is a root of $p$. Since all roots of $p$ are in $K$, $\sigma(a) \in K$.

The element $a$ has a minimal polynomial over $F$, with some degree $n$. By theorem 20.3 in Gallian, every element $b$ of $K = F(a)$ can be written as $b = c_0 + c_1 a + c_2 a^2 + \cdots + c_{n-1} a^{n-1}$ for some $c_i \in F$. Thus

$$\sigma(b) = \sum_{i=0}^{n-1} c_i (\sigma(a))^i \in K,$$

so $\sigma(K) \subseteq K$. ∎

**THEOREM 1.4.2 Fundamental Theorem of Galois Theory** Suppose $E$ is a splitting field over $F$ and $E \supseteq K \supseteq F$. Recall the two functions:

$$f(H) = E_H, \text{ if } H \leq G(E/F)$$
$$g(K) = G(E/K)$$

1. $f$ is a bijection, with inverse $g$, from the subgroups of $G(E/F)$ onto the subfields of $E$ that contain $F$. In other words, $K = E_{G(E/K)}$ and $H = G(E/E_H)$.
2. $[E : K] = |G(E/K)|$ and $[K : F] = |G(E/F)|/|G(E/K)|$.
3. $K$ is a normal extension of $F$ iff $G(E/K)$ is a normal subgroup of $G(E/F)$.
4. If $K$ is a normal extension of $F$, then $G(K/F) \cong {}^{G(E/F)}\!/_{G(E/K)}$.

***Proof.*** **1)** Suppose $E \supseteq K \supseteq F$. Since $E$ is a splitting field over $F$, it is also a splitting field over $K$. Hence $E$ is a normal extension of $K$ and so by definition of normal, $K = E_{G(E/K)}$. By theorem 1.3.2, if $H \leq G(E/F)$ then $H = G(E/E_H)$.

**2)** Suppose $E \supseteq K \supseteq F$. Again by theorem 1.3.2, $[E : F] = |G(E/F)|$ and $[E : K] = |G(E/K)|$. Then $|G(E/F)| = [E : F] = [E : K][K : F] = |G(E/K)|[K : F]$, so $[K : F] = |G(E/F)|/|G(E/K)|$.

**3)** By lemma 1.4.1, $K$ is a normal extension of $F$ iff

$$\forall \sigma \in G(E/F) \forall t \in K \big(\sigma(t) \in K\big). \tag{1.4.1}$$

Because $E$ is a normal extension of $K$, the fixed field of $G(E/K)$ is $K$, so condition 1.4.1 is equivalent to

$$\forall \sigma \in G(E/F) \forall \tau \in G(E/K) \forall t \in K \left(\tau\big(\sigma(t)\big) = \sigma(t)\right). \tag{1.4.2}$$

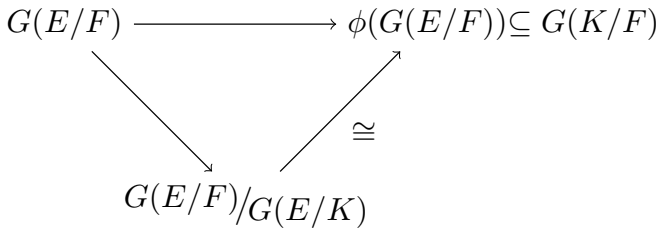
Condition 1.4.2 is equivalent to

$$\forall \sigma \in G(E/F) \forall \tau \in G(E/K) \forall t \in K (\sigma^{-1}(\tau(\sigma(t))) = t),$$

which means $\sigma^{-1}\tau\sigma$ fixes $K$, or $\sigma^{-1}\tau\sigma \in G(E/K)$. By theorem 9.1 in Gallian, this is equivalent to $G(E/K) \triangleleft G(E/F)$.

**4)** Suppose $K$ is a normal extension of $F$. Let $\sigma \in G(E/F)$, and denote the restriction of $\sigma$ to $K$ by $\overline{\sigma}$. By lemma 1.4.1, $\sigma(K) \subseteq K$, so $\overline{\sigma}$ is an isomorphism to a subfield of $K$. Viewing $K$ as a finite dimensional vector space, we have an isomorphism to a subspace of $K$ with the same dimension as $K$, so $\overline{\sigma}(K) = K$ and $\overline{\sigma} \in G(K/F)$. Since $\overline{\sigma \circ \tau} = \overline{\sigma} \circ \overline{\tau}$, the mapping $\sigma \mapsto \overline{\sigma}$ is a homomorphism, $\phi$, from $G(E/F)$ to $G(K/F)$.

The kernel of $\phi$ consists of those $\sigma$ such that $\overline{\sigma}$ is the identity automorphism on $K$, that is, such that $\sigma$ fixes $K$. Thus, the kernel is precisely $G(E/K)$. By part (3), $G(E/K) \triangleleft G(E/F)$, and by the First Isomorphism Theorem for Groups, $G(E/F)/G(E/K)$ is isomorphic to the range of $\phi$.




We know that

$$|G(K/F)| = [K : F] = \left|G(E/F)/G(E/K)\right| = \left|\phi\big(G(E/F)\big)\right|.$$

Thus the range of $\phi$ is a subgroup of $G(K/F)$ with the same size as $G(K/F)$, so the range is $G(K/F)$, which finishes the proof. ∎

# 2

# Solvability

## 2.1 Solvability by radicals

**DEFINITION 2.1.1** Let $f \in F[x]$, $F$ a field. $f$ is solvable by radicals over $F$ if there are elements $a_i$ and $n_i$ such that

$$F = F_0 \subseteq F(a_1) = F_1 \subseteq F_1(a_2) = F_2 \subseteq \cdots \subseteq F_{r-1}(a_r) = F_r,$$

$a_i^{n_i} \in F_{i-1}$, and $f$ splits in $F_r$. Each of the fields $F_i$ is called a radical extension of $F$. □

When $f$ is solvable by radicals, we can choose the fields $F_i$ with some nice additional properties. We see how to do this next.

An $n$th *root of unity* is any root of $x^n - 1$. We say $\omega$ is a *primitive* root of unity if $\{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ is the set of all of the $n$th roots of unity. Let $\omega_i$ be a primitive $i$th root of unity. Note that if $\mathbb{C} \supseteq F \supseteq \mathbb{Q}$, then $F(\omega_i)$ is the splitting field of $x^i - 1$ over $F$.

Suppose that $f$ is solvable by radicals, and suppose that the fields $J_i$, elements $b_i$ and exponents $m_i$, for $i = 1, \ldots, s$, are as described by the definition. Let $n$ be the maximum of all of the exponents $m_i$ of the definition, and form the following chain of fields:

$$\begin{aligned} F(\omega_3) = & L_1 \subseteq L_1(\omega_4) = L_2 \subseteq \cdots \subseteq L_{n-3}(\omega_n) = L_{n-2} = K_0 \subseteq \\ & K_0(b_1) = K_1 \subseteq K_1(b_2) = K_2 \subseteq \cdots \subseteq K_{s-1}(b_s) = K_s. \end{aligned}$$

Rename the fields $L_i$ and $K_i$ as a single sequence $F_i$, $i = 1, \ldots, r$, where $r = n - 2 + s$; rename the elements $\omega_3, \ldots, \omega_n, b_1, \ldots, b_s$ as $a_1, \ldots, a_r$; and rename the integers

$3, 4, \ldots, n, m_1, \ldots, m_s$ as $n_1, \ldots, n_r$. Then $f$ splits in $F_r$, $a_i^{n_i} \in F_{i-1}$, and

$$F = F_0 \subseteq F(a_1) = F_1 \subseteq F_1(a_2) = F_2 \subseteq \cdots \subseteq F_{r-1}(a_r) = F_r.$$

**LEMMA 2.1.2** Each of the fields $F_i$ just described is a normal extension of the preceding field, $F_{i-1}$.

***Proof.*** This is certainly true when the corresponding $a_i$ is a primitive root of unity. Otherwise, note that $a_i$ is a root of $x^{n_i} - a_i^{n_i} \in F_{i-1}[x]$. Let $\omega = \omega_{n_i}$ and consider the set $\{a_i, \omega a_i, \omega^2 a_i, \ldots, \omega^{n_i - 1} a_i\}$. Each of these elements is in $F_i$, each is a root of $x^{n_i} - a_i^{n_i}$, and they are distinct. Thus, $x^{n_i} - a_i^{n_i}$ splits in $F_i = F_{i-1}(a_i)$, so $F_i$ is the splitting field of $x^{n_i} - a_i^{n_i}$ over $F_{i-1}$ and by theorem 1.3.4, $F_i$ is a normal extension of $F_{i-1}$. ∎

**LEMMA 2.1.3** $G(F_i/F_{i-1})$ is abelian.

***Proof.*** There are two cases, depending on whether $a_i$ is a primitive root of unity or not. We do just the latter case; the former is similar. Remember that the roots of unity are all added first, so they are all in $F_{i-1}$.

Suppose that $\sigma \in G(F_i/F_{i-1})$. Since $a_i^{n_i} \in F_{i-1}$, $\sigma(a_i^{n_i}) = a_i^{n_i}$, so $(\sigma(a_i))^{n_i} - a_i^{n_i} = \sigma(a_i^{n_i} - a_i^{n_i}) = 0$, or in other words, $\sigma(a_i)$ is a root of $x^{n_i} - a_i^{n_i}$. By the proof of the previous lemma, $\sigma(a_i) = \omega_{n_i}^{j(\sigma)} a_i$ for some integer $j(\sigma)$. Now if $\tau \in G(F_i/F_{i-1})$,

$$\begin{aligned}(\sigma \circ \tau)(a_i) =& \sigma(\omega_{n_i}^{j(\tau)} a_i) = \omega_{n_i}^{j(\tau)} \sigma(a_i) = \omega_{n_i}^{j(\tau)} \omega_{n_i}^{j(\sigma)} a_i = \\ & \omega_{n_i}^{j(\sigma)} \omega_{n_i}^{j(\tau)} a_i = \omega_{n_i}^{j(\sigma)} \tau(a_i) = \tau(\omega_{n_i}^{j(\sigma)} a_i) = (\tau \circ \sigma)(a_i).\end{aligned}$$

Thus for all $\sigma$ and $\tau$ in $G(F_i/F_{i-1})$, $\sigma\tau$ and $\tau\sigma$ agree on $a_i$.

By theorem 20.3 in Gallian, every $b \in F_i$ can be written as $\sum c_j a_i^j$, where $c_j \in F_{i-1}$. Then

$$(\sigma\tau)(b) = \sum c_j ((\sigma\tau)(a_i))^j = \sum c_j ((\tau\sigma)(a_i))^j = (\tau\sigma)(b).$$

Thus, $\sigma\tau = \tau\sigma$ and so $G(F_i/F_{i-1})$ is abelian as desired. ∎

It need not be the case that $F_r$ is a normal extension of $F$, but we can produce a new tower of fields with the properties we already have verified, and with the additional property that the ultimate field is a normal extension of $F$.

**LEMMA 2.1.4** We may assume that $F_r$ is a normal extension of $F$.

***Proof.*** Let $g_i$ be the minimal polynomial for $a_i$ over $F$, and let $b_i$, $1 \leq i \leq s$ be a list of all roots of all of the $g_i$, that is, $s$ is the sum of the degrees of the $g_i$. For convenience,

let $b_1, \ldots, b_r$ be $a_1, \ldots, a_r$. Let $N$ be the splitting field of the product $g = \prod g_i$, that is, $N = F(b_1, \ldots, b_s) \supseteq F_r$. We will extend the tower of fields:

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r \subseteq F_{r+1} \subseteq \cdots \subseteq F_m = N.$$

For each root $b_i$ of $g_k$, there is an isomorphism $\sigma_i \colon F(a_k) \to F(b_i)$ that fixes $F$, by the lemma on page 348 in Gallian. By theorem 20.4, $\sigma_i$ may be extended to an automorphism $\overline{\sigma}_i$ on the splitting field $N$ that fixes $F$(note that $\sigma_i(g) = g$). Now $\overline{\sigma}_i(F_r)$ is a subfield of $N$ that contains $b_i$ and is isomorphic to $F_r$; in particular, $\overline{\sigma}_i(F_r)$ may be viewed as arising from a tower of fields formed using the elements $\overline{\sigma}_i(a_j)$, $1 \leq j \leq r$, and $\overline{\sigma}_i(F_j) = \overline{\sigma}_i(F(a_1, \ldots, a_j)) = F(\overline{\sigma}_i(a_1), \ldots, \overline{\sigma}_i(a_j))$.

Thus, for each root $b_i$ we have a corresponding sequence of elements $\overline{\sigma}_i(a_j) = a_{i,j}$, $1 \leq j \leq r$, one of which is $b_i$. Then we see that $N = F(a_1, a_2, \ldots, a_r, a_{r+1,1}, a_{r+1,2}, \ldots, a_{s,r})$, and

$$\begin{aligned} F =& F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r \subseteq N_{r+1,1} = F_r(a_{r+1,1}) \subseteq N_{r+1,2} = N_{r+1,1}(a_{r+1,2}) \subseteq \cdots \\ & \subseteq N_{s,r-1} = N_{s,r-2}(a_{s,r-1}) \subseteq N_{s,r} = N_{s,r-1}(a_{s,r}) = N. \end{aligned}$$

Note that we add all of the elements $\{a_{i,1}, a_{i,2}, \ldots, a_{i,r}\}$ just to get $b_i = a_{i,k}$; we do this so that each field is obtained from the previous one by adding a root. Now we need to verify that each $a_{i,j}$ is a root of some element in the previous field. There are two cases:

$j = 1$: We need to show some power of $a_{i,1}$ is in $N_{i-1,r}$, or $F_r$ if $i = r+1$. If $i = r+1$,

$$a_{i,1}^{n_1} = (\overline{\sigma}_i(a_1))^{n_1} = \overline{\sigma}_i(a_1^{n_1}) \in \overline{\sigma}_i(F) = F \subseteq F_r,$$

else

$$a_{i,1}^{n_1} = (\overline{\sigma}_i(a_1))^{n_1} = \overline{\sigma}_i(a_1^{n_1}) \in \overline{\sigma}_i(F) = F \subseteq N_{i-1,r}.$$

$j > 1$: We need to show some power of $a_{i,j}$ is in $N_{i,j-1}$:

$$\begin{aligned} a_{i,j}^{n_j} &= (\overline{\sigma}_i(a_j))^{n_j} = \overline{\sigma}_i(a_j^{n_j}) \in \overline{\sigma}_i(F_{j-1}) = \overline{\sigma}_i(F(a_1, \ldots, a_{j-1})) \\ &= F(\overline{\sigma}_i(a_1), \ldots, \overline{\sigma}_i(a_{j-1})) = F(a_{i,1}, \ldots, a_{i,j-1}) \subseteq N_{i,j-1}. \end{aligned}$$

■

By the Fundamental Theorem, $G(F_r/F_{i+1}) \triangleleft G(F_r/F_i)$ and

$$G(F_{i+1}/F_i) \cong G(F_r/F_i)/G(F_r/F_{i+1}),$$

and by lemma 2.1.3, this group is abelian. So we have a tower of groups:

$$\{\epsilon\} = G(F_r/F_r) \triangleleft G(F_r/F_{r-1}) \triangleleft \cdots \triangleleft G(F_r/F_{i+1}) \triangleleft G(F_r/F_i) \triangleleft \cdots \triangleleft G(F_r/F),$$

in which each factor group $G(F_r/F_i)/G(F_r/F_{i+1})$ is abelian. It's not obvious that this property of $G(F_r/F)$ is special, but in fact it is, and deserves a definition.

**DEFINITION 2.1.5** $G$ is a solvable group if there are subgroups $H_i$ of $G$ such that

$$\{e\} = H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_k = G$$

and such that all factor groups $H_{i+1}/H_i$ are abelian. □

Remember that we are investigating what it means for a polynomial $f$ to be solvable by radicals. Although $f$ splits in $F_r$, $F_r$ is likely to be much larger than the splitting field of $f$, and it is not obvious that a property held by $F_r$ has much to say about $f$. Let $E$ be the splitting field for $f$ over $F$, so $F \subseteq E \subseteq F_r$. Since $E$ is a normal extension of $F$, the Fundamental Theorem says

$$G(E/F) \cong {}^{G(F_r/F)}\!/_{G(F_r/E)},$$

so $G(E/F)$ is a factor group of a solvable group.

**LEMMA 2.1.6** A factor group of a solvable group is solvable.

***Proof.*** Let $H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_k = G$ be a tower of groups that illustrates that $G$ is solvable, and let $N \lhd G$. Consider the groups

$$H_0N/N \subseteq H_1N/N \subseteq \cdots \subseteq H_kN/N = G/N.$$

Suppose that $x \in H_i$, $y \in H_{i+1}$, $n, m \in N$, $xnN = xN \in H_iN/N$, $ymN = yN \in H_{i+1}N/N$. Then $yNxN(yN)^{-1} = yxy^{-1}N$. Since $H_i \lhd H_{i+1}$, $yxy^{-1} \in H_i$, so $yxy^{-1}N \in H_iN/N$ and $H_iN/N \lhd H_{i+1}N/N$.

Now consider two elements of $(H_{i+1}N/N)/(H_iN/N)$, $(gnN)(H_iN/N) = (gN)(H_iN/N)$ and $(hmN)(H_iN/N) = (hN)(H_iN/N)$. We want to show these elements commute, that is, $(ghN)(H_iN/N) = (hgN)(H_iN/N)$. It suffices to show that $(hgN)^{-1}(ghN) = g^{-1}h^{-1}ghN \in H_iN/N$. Since $H_{i+1}/H_i$ is abelian, $g^{-1}h^{-1}gh \in H_i$, this is true. ■

To show that some polynomial $f$ is not solvable by radicals, it is therefore sufficient to show that $G(E/F)$ is not solvable, where $E$ is the splitting field of $f$. We will show that for $f = 3x^5 - 15x + 5$, $G(E/F) = S_5$, and that $S_n$ is not solvable when $n \geq 5$.

## 2.2 Unsolvability of $S_n$

**DEFINITION 2.2.1** Let $U(G)$ be the set of commutators of the group $G$:

$$U(G) = \{xyx^{-1}y^{-1} | x, y \in G\}.$$

The commutator subgroup of $G$, denoted $G'$, is the smallest subgroup containing $U(G)$, that is, $G' = \langle U(G) \rangle$. □

**LEMMA 2.2.2** If $X$ is any subset of $G$ and for all $g \in G$, $gXg^{-1} \subseteq X$, then $\langle X \rangle$ is a normal subgroup of $G$.

***Proof.*** Note that the hypothesis implies that for all $g \in G$, $X \subseteq g^{-1}Xg$. Suppose that $y \in \langle X \rangle$; we need to show that for all $g \in G$, $gyg^{-1} \in \langle X \rangle$. Let $H = g^{-1}\langle X \rangle g$; $H$ is a subgroup of $G$, called a conjugate of $\langle X \rangle$ (see problem 1, page 91 in Gallian). Since $H = g^{-1}\langle X \rangle g \supseteq g^{-1}Xg \supseteq X$, $H$ is a subgroup containing $X$ and therefore $H \supseteq \langle X \rangle$, so $y \in H$. Now $gyg^{-1} \in gHg^{-1} = gg^{-1}\langle X \rangle gg^{-1} = \langle X \rangle$. ■

**LEMMA 2.2.3** $G' \triangleleft G$.

***Proof.*** It suffices to check that $gU(G)g^{-1} \subseteq U(G)$, that is, that for any $x$, $y$, and $g$ in $G$, $gxyx^{-1}y^{-1}g^{-1}$ is a commutator. Write

$$\begin{aligned} gxyx^{-1}y^{-1}g^{-1} &= (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) \\ &= uvu^{-1}v^{-1}, \end{aligned}$$

where $u = gxg^{-1}$ and $v = gyg^{-1}$. ■

**LEMMA 2.2.4** $G/G'$ is abelian.

***Proof.*** We need to show that $xyG' = yxG'$ for all $x$ and $y$ in $G$. By properties of cosets, this is true if and only if $(yx)^{-1}xy \in G'$. This is true because $(yx)^{-1}xy = x^{-1}y^{-1}xy \in U(G) \subseteq G'$. ■

**LEMMA 2.2.5** If $H \triangleleft G$ and $G/H$ is abelian, then $H \supseteq G'$.

***Proof.*** For any $x$ and $y$ in $G$, $xyH = yxH$, so $x^{-1}y^{-1}xyH = H$ or $x^{-1}y^{-1}xy \in H$—that is, $H$ contains every commutator, so $H \supseteq G'$. ■

**DEFINITION 2.2.6** $G^{(0)} = G$ and $G^{(k)} = \left(G^{(k-1)}\right)'$ for $k \geq 1$. □

**THEOREM 2.2.7** $G$ is solvable iff $G^{(k)} = \{e\}$ for some $k$.

***Proof.*** If $G^{(k)} = \{e\}$ then $\{e\} = G^{(k)} \triangleleft G^{(k-1)} \triangleleft \cdots \triangleleft G'' \triangleleft G' \triangleleft G$ and $G^{(i-1)}/G^{(i)}$ is abelian.

Suppose $\{e\} = N_k \triangleleft N_{k-1} \triangleleft \cdots \triangleleft N_1 \triangleleft N_0 = G$ and $N_i/N_{i+1}$ is abelian. By lemma 2.2.5, $N_1 \supseteq G'$, $N_2 \supseteq N_1' \supseteq G''$, and by an easy induction, $N_k \supseteq G^{(k)}$, so $\{e\} = G^{(k)}$. ■

**LEMMA 2.2.8** $G^{(i)} \triangleleft G$ for all $i$.

***Proof.*** Suppose that $N \triangleleft G$; we prove that $N' \triangleleft G$. Suppose $g \in G$ and $u \in N'$; we need to prove that $gug^{-1} \in N'$. By lemma 2.2.2, it suffices to prove that if $u \in U(N)$

then $gug^{-1} \in U(N)$. This is almost identical to the proof of lemma 2.2.3. Now an easy induction completes the proof. ∎

**LEMMA 2.2.9** Let $G = S_n$, $n \geq 5$. For every $k$, $G^{(k)}$ contains every 3-cycle in $S_n$.

***Proof.*** Suppose $N \triangleleft G$ and $N$ contains all 3-cycles, so $N'$ contains the commutator $(123)(145)(321)(541) = (124)$. $N'$ is normal in $G$, so for all $\pi \in S_n$, $\pi(124)\pi^{-1} \in N'$. Choose $\pi$ so that $\pi(1) = i$, $\pi(2) = j$, $\pi(4) = k$. Then $(ijk) = \pi(124)\pi^{-1}$, so every 3-cycle is in $N'$.

Now we prove the lemma by induction on $k$. $G \triangleleft G$ and $G$ contains all 3-cycles, so $G'$ contains all 3-cycles. By the induction hypothesis, $G^{(k)}$ contains all 3-cycles. By the previous lemma, $G^{(k)} \triangleleft G$, so $G^{(k+1)} = \left(G^{(k)}\right)'$ contains all 3-cycles. ∎

**THEOREM 2.2.10** $S_n$ is not solvable when $n \geq 5$.

***Proof.*** If $S_n$ is solvable then for some $k$, $G^{(k)} = \{e\}$. But also $G^{(k)}$ contains all 3-cycles, a contradiction. ∎

## 2.3 Unsolvability of the quintic

The polynomial $f = 3x^5 - 15x + 5$ is irreducible over the rationals, by Eisenstein's criterion. By 20.6 in Gallian, it has no multiple roots, and by the Fundamental Theorem of Algebra (i.e., $\mathbb{C}$ is algebraically closed), it has 5 distinct roots in $\mathbb{C}$. It is not hard to see that $f$ has exactly 3 real roots, so it also has roots $a \pm bi$ for some $a$ and $b$, by problem 65 in chapter 15 of Gallian.

Denote the roots of $f$ by $r_1, \ldots, r_5$, so the splitting field of $f$ is $\mathbb{Q}(r_1, \ldots, r_5) = \mathbb{Q}(\overline{r})$. Any $\sigma \in G(\mathbb{Q}(\overline{r})/\mathbb{Q})$ permutes the roots $r_i$, and in fact $\sigma$ is completely determined by its action on the roots. In other words, $G(\mathbb{Q}(\overline{r})/\mathbb{Q}) \leq S_5$ (there is of course a hidden isomorphism here). Since $[\mathbb{Q}(\overline{r}) : \mathbb{Q}] = [\mathbb{Q}(\overline{r}) : \mathbb{Q}(r_1)][\mathbb{Q}(r_1) : \mathbb{Q}] = [\mathbb{Q}(\overline{r}) : \mathbb{Q}(r_1)] \cdot 5$, $[\mathbb{Q}(\overline{r}) : \mathbb{Q}] = |G(\mathbb{Q}(\overline{r})/\mathbb{Q})|$ is divisible by 5.

**LEMMA 2.3.1** If $p$ is prime and $p$ divides $|G| = n$, then $G$ has an element of order $p$.

***Proof.*** What elements of $G$ are solutions to $x^p = 1$? Certainly $x = 1$ is a root. If $y \neq 1$ is a solution, then $y$ has order $p$, so it suffices to show that there are at least 2 solutions.

Let $S = \{(a_1, \ldots, a_p) | \prod a_i = 1\}$. For any choice of $a_1, \ldots, a_{p-1}$, there is a unique $a_p$ such that $(a_1, \ldots, a_p)$ is in $S$, so $|S| = n^{p-1}$. If $\overline{a}$ and $\overline{b}$ are in $S$, say $\overline{a} \equiv \overline{b}$ if each may be obtained by rotating the other—for example, $(a_1, \ldots, a_p) \equiv (a_3, \ldots, a_p, a_1, a_2)$. If $a_i = a_j$ for all $i$ and $j$, then $(a_1, \ldots, a_p)$ forms an entire equivalence class. Otherwise, since $p$ is prime, there must be exactly $p$ members of each equivalence class. Each solution $c$ of $x^p = 1$ corresponds to an equivalence class $\{(c, c, c, \ldots, c)\}$, and vice versa, so the number

of solutions is equal to the number of one element equivalence classes, say $r$. Let $s$ be the number of $p$-element equivalence classes. Then $n^{p-1} = r + sp$. By hypothesis $p|n$, so $p|r$. Since $r \geq 1$, this means $r \geq 2$ as desired. ■

Returning to $G(\mathbb{Q}(\overline{r})/\mathbb{Q})$, we now see that this group contains an element of order 5, which must be a 5-cycle. Let $\sigma\colon \mathbb{C} \to \mathbb{C}$ be defined by $\sigma(x + yi) = x - yi$; $\sigma$ is an automorphism (example 2, chapter 15). Since $\sigma$ permutes the roots of $f$, its restriction to $\mathbb{Q}(\overline{r})$ is in $G(\mathbb{Q}(\overline{r})/\mathbb{Q})$, and clearly $\sigma$ has order 2. Thus, $G(\mathbb{Q}(\overline{r})/\mathbb{Q})$ contains both a 2-cycle and a 5-cycle. Without loss of generality we may assume that $G(\mathbb{Q}(\overline{r})/\mathbb{Q})$ contains (12) and (12345). Finally, it is a bit tedious but not difficult to prove that if $H$ is a subgroup of $S_5$ and $H$ contains (12) and (12345), then $H = S_5$, so in fact $G(\mathbb{Q}(\overline{r})/\mathbb{Q}) \cong S_5$. Since $S_5$ is not solvable, $f$ is not solvable by radicals. Since this particular quintic is not solvable by radicals, it is clear also that there can be no "formula" for the roots of a quintic.

In fact, not even one of the roots may be written as an expression in radicals, since if it could, we could divide out the corresponding linear factor and then solve the resulting quartic completely, giving a complete solution of the quintic in radicals. This argument works only for fifth degree polynomials; here is a more general way to talk about individual roots.

**THEOREM 2.3.2** Suppose $f \in F[x]$ has roots $r_1, \ldots, r_n$, and that for all $i$, $F(r_1) \cong F(r_i)$, by an isomorphism $\sigma_i$ that fixes $F$. If there is a radical extension of $F$ containing $F(r_1)$ then there is a radical extension of $F$ in which $f$ splits, that is, $f$ is solvable by radicals.

***Proof.*** Let $F_i = F_{i-1}(a_i)$, $i = 1, \ldots, s$, be the tower of fields forming the radical extension containing $F(r_1)$. Let $g_i$ be the minimal polynomial of $a_i$ over $F$, and let $g = f \prod g_i$. Let $N$ be the splitting field of $g$ over $F$. By theorem 20.4 in Gallian, the isomorphism $\sigma_i$ from $F(r_1)$ to $F(r_i)$ can be extended to an automorphism on $N$. Then $\sigma_i(F_s)$ is a radical extension containing $F(r_i)$, formed using the elements $\sigma_i(a_j)$. As in lemma 2.1.4, each of the other roots of $g$ is also contained in a copy of $F_s$, and we may put all of these radical extensions together into a single tower of fields culminating in $N$. Thus $N$ is a radical extension of $F$ that contains the splitting field of $f$, as desired. ■

So as long as the roots of a polynomial "look alike," if one of them can be written as an expression in radicals, all of them can and the corresponding Galois group is solvable. In particular, if the Galois group is $S_n$, $n \geq 5$, then the roots are individually not expressible by radicals.

## 2.4 No formula for roots

We have seen that for $F = \mathbb{Q}$ there is a specific fifth degree polynomial that is not solvable by radicals. This implies that there can be no formula for the roots of polynomials of degree greater than or equal to five, where by "formula" we mean an expression using the four simple arithmetic operations and arbitrary $k$th roots.

We can show directly that no such formula is possible, for any $F$ of characteristic 0. Consider the "general" polynomial $f(t) = t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n$, $n \geq 5$. A formula for a root of $f(t)$ would be an expression containing the symbols $a_i$ as placeholders for elements of $F$. We may instead interpret $f(t)$ as a specific polynomial in $F(a_1, \ldots, a_n)$, the field of rational functions in the symbols $a_i$. Now the question is whether $f(t)$ is solvable by radicals over $F(a_1, \ldots, a_n)$.

Let $E$ be a splitting field for $f(t)$, so in $E$

$$\prod_{i=1}^{n} (t - x_i) = f(t).$$

Then $E = F(x_1, \ldots, x_n)$ and the coefficients $a_i$ are the elementary symmetric functions in the $x_i$. As we saw in theorem 1.2.3, $G(E/F(\overline{a})) \cong S_n$. Since $S_n$ is not solvable, $f(t)$ is not solvable by radicals over $F(\overline{a})$, so there can be no formula for any root of $f(t)$.

# Index