AN INTRODUCTION TO GALOIS THEORY

STEVEN DALE CUTKOSKY

In these notes we consider the problem of constructing the roots of a polynomial. Suppose that F is a subfield of the complex numbers, and $f(x)$ is a polynomial over F. We wish to give a *rational formula for constructing the roots of* $f(x)$. The quadratic formula is an example of such a formula.

Let $f(x) = ax^2 + bx + c$, where $a \neq 0$. We make the substitution $y = x + \frac{b}{2a}$ to obtain the equation

$$y^2 = \frac{b^2}{4a^2} - \frac{c}{a},$$

which yields a formula for the two roots of $f(x)$,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

This formula was known in ancient times, while formulas for solving cubic and quadric equations where discovered in the Renaissance.

Suppose that $f(x) = ax^3 + bx^2 + cx + d$, with $a \neq 0$. We first make the substitution $y = x + \frac{b}{3a}$ to obtain the equation

$$y^3 + py + q = 0$$

(with $p = \frac{c}{a} - \frac{b^2}{3a^2}$, $q = \frac{d}{a} - \frac{bc}{3a^2} + \frac{2b^3}{27a^3}$). Now make the substitution $y = z - \frac{p}{3z}$ to obtain

$$z^3 - \frac{p^3}{27z^3} + q = 0.$$

We multiply the equation by z^3 and use the quadratic formula to obtain

$$z^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Taking cube roots, we obtain six solutions for z. Substituting into $y = z - \frac{p}{3z}$ we obtain 3 distinct solutions.

Next, we solve the quartic equation. Suppose that $f(x) = ax^4 + bx^3 + cx^2 + dx + e$ with $a \neq 0$. substitute $z = x + \frac{b}{4a}$ to obtain the equation

$$z^4 + pz^2 + qz + r = 0.$$

For all $u \in \mathbb{C}$, this expression is equal to

$$z^4 + z^2u + \frac{u^2}{4} - z^2u - \frac{u^2}{4} + pz^2 + qz + r = 0, \tag{1}$$

or

$$(z^2 + \frac{u}{2})^2 - [(u-p)z^2 - qz + (\frac{u^2}{4} - r)] = 0.$$

Date: November 16, 2009.

Let $P = z^2 + \frac{u}{2}$. The quadratic polynomial $(u-p)z^2 - qz + (\frac{u^2}{4} - r)$ is of the form Q^2, where Q is a linear polynomial in z, precisely when the discriminant of $(u-p)z^2 - qz + (\frac{u^2}{4} - r)$ is zero. This occurs for values of u such that

$$q^2 = 4(u-p)(\frac{u^2}{4} - r).$$

Solving this cubic equation for u, we set u to be a root of this equation, so that (1) has the form $0 = P^2 - Q^2 = (P+Q)(P-Q)$, or

$$(z^2 + \frac{u}{2} + L)(z^2 + \frac{u}{2} - L) = 0 \tag{2}$$

where L is a linear function of z. Equation (2) is a product of two quadratic equations, each of which can be solved for z using the quadratic formula. We have thus obtained the solutions to our quartic equation $f(x)$.

At this point, one may wonder if, with sufficient cleverness, it may be possible to solve fifth and higher degree equations. This is actually not the case, as was discovered only in the nineteenth century, by Abel, Ruffini and Galois. The remainder of these notes will be devoted to proving the insolvability of higher degree equations.

All rings R will be assumed to have a multiplicative identity 1_R. We will denote 1_R by 1 when there is no danger of confusion. All ring homomorphisms $\Phi : R \to S$ will be required to satisfy $\Phi(1_R) = 1_S$. In particular, if R is a field, then Φ is 1-1.

Suppose that R, S are commutative rings (with identity), and U is a subset of S. We define the subring of S generated by R and U by

$$R[U] = \{\sum_{i_1=0}^{r_1} \cdots \sum_{r_n=0}^{r_n} a_{i_1 \cdots i_n} u_1^{i_1} \cdots u_n^{i_n} \mid n \in \mathbb{N}, u_1, \ldots, u_n \in U, r_1, \ldots, r_n \in \mathbb{N} \text{ and } a_{i_1 \cdots i_n} \in R\}.$$

If $U = \{u\}$,

$$R[u] = \{\sum_{i=0}^{r} a_i u^i \mid r \in \mathbb{N} \text{ and } a_i \in R\}.$$

Suppose that K is a subfield of a field L, and U is a subset of L. We define the subfield of L generated by K and U to be

$$K(U) = \{\frac{f}{g} \mid f, g \in K[U] \text{ and } g \neq 0\}.$$

The polynomial ring in the indeterminates $\{x_1, \ldots, x_n\}$ is a ring $R[x_1, \ldots, x_n]$ generated by R and the set $\{x_1, \ldots, x_n\}$ which has the property that for a polynomial with coefficients $a_{i_1 \cdots i_n} \in R$,

$$f(x_1, \ldots, x_n) = \sum_{i_1=0}^{r_1} \cdots \sum_{r_n=0}^{r_n} a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} = 0$$

if and only if all coefficients $a_{i_1 \cdots i_n} = 0$.

The polynomial ring $R[x_1, \ldots, x_n]$ has the following universal property.

Theorem 0.1. *Suppose that $\Phi : R \to S$ is a ring homomorphism (of commutative rings with identity), and $u_1, \ldots, u_n \in S$. Then there is a unique ring homomorphism $\overline{\Phi} : R[x_1, \ldots, x_n] \to S$ such that $\overline{\Phi}(r) = r$ for $r \in R$ and $\overline{\Phi}(x_i) = u_i$ for $1 \leq i \leq n$.*

Suppose that F is a subfield of a field K, and $u \in K$. u is called algebraic over F if there exist a positive integer n and $a_0, a_1, \ldots, a_n \in F$ not all zero such that $a_0 + a_u + \cdots + a_n u^n = 0$. u is called transcendental over F if u is not algebraic over F.

By the universal property of polynomial rings, there is a surjective ring homomorphism

$$\Psi : F[x] \to F[u]$$

such that $\Psi(f(x)) = f(u)$ for $f(x) \in F[x]$. Let I be the kernel of Ψ. Since $F[x]$ is a PID, $I = (f) = \{fg \mid g \in F[x]\}$ for some $f \in F[x]$. By the first isomorphism theorem, $\overline{\Psi} : F[x]/I \to F[u]$ defined by $\overline{\Psi}(g + I) = \Psi(g)$ is a ring isomorphism. Since $F[u]$ is a domain, I is a prime ideal in $F[x]$ and thus either I is the zero ideal, or $f(x)$ is irreducible in $F[x]$.

There is a relation $a_0 + a_1 u + \cdots + a_n u^n = 0$ in $F[u]$ with n a nonnegative integer and $a_i \in F$ for all i if and only if the polynomial $g(x) = a_0 + a_1 x + \cdots + a_n x^n$ is in the kernel I of Ψ. Thus u is transcendental over F if and only if the Kernel I of Ψ is the zero ideal.

If u is transcendental over F, then $F[u]$ is (isomorphic to) a polynomial ring, so $F[u]$ is not a field. The field $F(u)$ generated by F and u is the rational function field

$$F(u) = \{\frac{f(x)}{g(x)} \mid f, g \in F[x] \text{ and } g \neq 0\}.$$

The statement that u is transcendental over F is equivalent to the statement that the set $\{u^i \mid i \in \mathbb{N}\}$ is a basis of $F[u]$.

Suppose that u is algebraic over F, so that the kernel I of Ψ is generated by an irreducible polynomial $f(x)$. Since the units in $F[x]$ are the nonzero elements of F, there is a unique monic polynomial $f(x)$ which generates I. A polynomial $f(x)$ is monic if its leading coefficient is 1. That is, $f(x)$ has an expression

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$$

for some $n \geq 1$. This unique monic polynomial $f(x)$ which generates the kernel I of Ψ is called the minimal polynomial of u.

We say that u is a root of a polynomial $g(x) \in F[x]$ if $g(u) = 0$ (or equivalently $g \in I$).

Theorem 0.2. *Suppose that F is a field and u is algebraic over F. Let $f(x)$ be the minimal polynomial of u over F. Then*

1. *$f(x)$ is the monic polynomial in $F[x]$ of smallest degree with the property that $f(u) = 0$.*
2. *f is irreducible in $F[x]$.*
3. *u is a root of $g(x) \in F[x]$ if and only if f divides g.*

The following criteria is useful for finding the minimal polynomial.

Corollary 0.3. *Suppose that F is a field and u is algebraic over F. A polynomial $f(x) \in F[x]$ is the minimal polynomial of u over F if and only if*

1. *u is a root of f.*
2. *f is monic and irreducible in $F[x]$*

Lemma 0.4. *Suppose that R is a domain which contains a field F such that R is a finite dimensional vector space over F. Then R is a field.*

Proof. Suppose $a \in R$ is a nonzero element. Define $T : R \to R$ by $T(b) = ab$ for $b \in R$. The kernel of T is $\{0\}$ since T is a domain. Since R is a finite dimensional vector space, T is onto by the rank nullity theorem. Thus there exists $b \in R$ such that $ab = 1$. □

Lemma 0.5. *Suppose that u is algebraic over F with minimal polynomial $f(x) \in F[x]$. Let $n = deg(f)$. Then $F[u]$ is an n-dimensional vector space over F. Further, $\{1, u, \ldots, u^{n-1}\}$ is an F-basis of F. Thus $F[u]$ is a field.*

Proof. Suppose that $\beta \in F[u]$. Then $\beta = g(u)$ for some polynomial $g(x) \in F[x]$. By Euclidean division, $g(x) = q(x)f(x) + r(x)$ where $q, r \in F[x]$ and $\deg(r) < n$. $\beta = g(u) = q(u)f(u) + r(u) = r(u)$. Thus $\{1, u, u^2, \ldots, u^{n-1}\}$ span $F[u]$ as a vector space over F. Suppose that there is a relation $a_0 + a_1u + a_2u^2 + \cdots + a_{n-1}u^{n-1} = 0$ for some $a_0, a_1, \ldots, a_{n-1} \in F$. Let $g(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in F[x]$. Since $g(u) = 0$, we have that f divides g in $F[x]$. If $g \neq 0$ we must then have that $n - 1 \geq \deg(g) \geq \deg(f) = n$, a contradiction. Thus we must have that $g = 0$, and we see that $\{1, u, \ldots, u^{n-1}\}$ are linearly independent over F and are thus a basis of $F[u]$. $F[u]$ is a field by Lemma 0.4. □

Definition 0.6. *Suppose that F is a subfield of a field K, so that K is a vector space over F. Denote the dimension of K as a vector space over F by $[K : F]$.*

Thus u is algebraic over F if and only if $[F[u] : F] < \infty$.

A useful criterion for irreducibility of polynomials of small degree is the following lemma.

Lemma 0.7. *Suppose that F is a field and $f(x) \in F[x]$ is a nonzero polynomial of degree 2 or 3. Then $f(x)$ is irreducible if and only if f has no root in F.*

Example 0.8. *The above criterion is not valid for polynomials of degree ≥ 4. A simple example is $f(x) = (x^2 + 1)^2 \in \mathbb{Q}[x]$ which has no root in $\mathbb{Q}$, but is not irreducible.*

Lemma 0.9. *Suppose that $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_i \in \mathbb{Z}$ and $a_n \neq 0$. Suppose that $\gamma \in \mathbb{Q}$ is a root of $f(x)$. Write $\gamma = \frac{\alpha}{\beta}$ where α, β are relatively prime integers. Then α divides a_0 and β divides a_n.*

Example 0.10. *$f(x) = x^2 + 1$ is the minimal polynomial of $\sqrt{-1}$ over $\mathbb{Q}$. $[\mathbb{Q}[i] : \mathbb{Q}] = 2$.*

The n-th roots of unity in a field F is the set $\{\xi \in F \mid \xi^n = 1\}$. In $\mathbb{C}$, the n-th roots of unity is the set $\{e^{\frac{m2\pi\sqrt{-1}}{n}} \mid 0 \leq m \leq n - 1\}$.

Example 0.11. *Suppose that p is a prime number. Let $\xi = e^{\frac{2\pi\sqrt{-1}}{p}} \in \mathbb{C}$. $\xi^p = 1$ so that ξ is a root of the polynomial $x^p - 1 \in \mathbb{Q}[x]$. $x^p - 1$ factors as the product*

$$x^p - 1 = (x^{p-1} + x^{p-2} + \cdots + x + 1)(x - 1)$$

in $\mathbb{Q}[x]$. Since $\xi - 1 \neq 0$, ξ is a root of the cyclotomic polynomial $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Since p is a prime, $f(x)$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion. Thus $f(x)$ is the minimal polynomial of ξ over $\mathbb{Q}$. $\mathbb{Q}[\xi] \cong \mathbb{Q}[x]/(f(x))$ and $[\mathbb{Q}[\xi] : \mathbb{Q}] = p - 1$.

Returning to Example 0.10, observe that $(\sqrt{-1})^4 = 1$ but $[\mathbb{Q}[\sqrt{-1}] : \mathbb{Q}] = 2$, not 3. This is because the cyclotomic polynomial $x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$ is not irreducible.

Lemma 0.12. *Suppose that $K \subset L \subset M$ are fields. Then $[M : K] = [M : L][L : K]$.*

Lemma 0.12 is proven by showing that if $\{u_i\}$ is a basis of L over K and $\{v_j\}$ is a basis of M over L, then $\{u_i v_j\}$ is a basis of M over K.

Definition 0.13. *Suppose that F is a field and $f(x) \in F[x]$ is a nonzero polynomial. An extension field E of F is a splitting field of $f(x)$ over F if the following two conditions hold:*

1. *$f(x)$ factors into a product of linear factors in $E[x]$. That is, there exist distinct elements $u_1, \ldots, u_k \in E$, a nonzero element $c \in F$ and positive integers $e_1, \ldots, e_k$ such that*

$$f(x) = c(x-u_1)^{e_1}(x-u_2)^{e_2}\cdots(x-u_k)^{e_k}. \tag{3}$$

2. *$E = F[u_1, \ldots, u_k]$ (so that E is generated by the roots of $f(x)$ and F).*

We say that f has multiple roots if some $e_i > 1$ in (3).

Theorem 0.14. *Suppose that F is a field and $f(x)$ is an irreducible polynomial in $F[x]$. Then there exists an extension field $K = F[\alpha]$ of F such that $f(\alpha) = 0$.*

Proof. Set $K = F[x]/(f(x))$. Let $\alpha = x + (f(x))$. We have $f(\alpha) = f(x) + (f(x)) = 0$. □

Theorem 0.15. *Suppose that F is a field, and $f(x) \in F[x]$ is a nonzero polynomial. Then there exists a splitting field E of $f(x)$ over F.*

Proof. We prove the theorem by induction on the degree of $f(x)$. Let $p(x)$ be an irreducible factor of $f(x)$ in $F[x]$. By Theorem 0.14 there exists an extension field $K = F[\alpha]$ of F such that α is a root of $p(x)$. Thus $f(x)$ is a product of the linear polynomial $(x-\alpha)$ and a polynomial $g(x) \in K[x]$. By induction, there exists a splitting field E of $g(x)$ over K. Thus E is a splitting field of $f(x)$ over F. □

Example 0.16. *Suppose that Suppose that $f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$ is irreducible. Then $b^2 - 4ac \neq 0$, so that f has two distinct roots*

$$u_1 = \frac{-b + \sqrt{b^2-4ac}}{2a} \text{ and } u_2 = \frac{-b - \sqrt{b^2-4ac}}{2a}$$

(where $\sqrt{b^2-4ac}$ is a choice of square root). $K = \mathbb{Q}[u_1, u_2]$ is a splitting field of $f(x)$ over $\mathbb{Q}$. We have $K = \mathbb{Q}[u_1]$ since $u_2 = -u_1 - \frac{b}{a} \in \mathbb{Q}[u_1]$. $[K : \mathbb{Q}] = 2$ since $\mathbb{Q}[u_1] \cong \mathbb{Q}[x]/(f(x))$.

Example 0.17. *Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Let $u = \sqrt[3]{2}$ be the (unique) real cube root of 2. Let $\omega = e^{\frac{2\pi\sqrt{-1}}{3}}$. $f(x) = (x-u)(x-\omega u)(x-\omega^2 u)$ in $\mathbb{C}[x]$. Thus $K = \mathbb{Q}[u, \omega u, \omega^2 u] = \mathbb{Q}[u, \omega]$ is a splitting field of $f(x)$ over $\mathbb{Q}$. Observe that $\mathbb{Q}[u]$ is not equal to K, since $\mathbb{Q}[u]$ is contained in $\mathbb{R}$, which does not contain ω. As $f(x)$ has degree 3 and has no root in $\mathbb{Q}$, $f(x)$ is irreducible in $\mathbb{Q}[x]$ and is the minimal polynomial of u over $\mathbb{Q}$. Thus $\mathbb{Q}[u] \cong \mathbb{Q}[x]/(x^3-2)$, so $[\mathbb{Q}[u] : \mathbb{Q}] = 3$. Let $L = \mathbb{Q}[u]$. $x^2 + x + 1 = (x-\omega)(x-\omega^2)$. $x^2 + x + 1$ is irreducible in $L[x]$ since $x^2 + x + 1$ has degree 2 and $x^2 + x + 1$ does not have a root in L. Thus $K = L[\omega] \cong L[x]/(x^2 + x + 1)$, and $[K : L] = 2$. We have $[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}] = 6$.*

Example 0.18. *Let $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. $f(0) = f(1) = 1$ so f has no roots in $\mathbb{Z}_2$. Since f has degree 3, $f(x)$ is irreducible in $\mathbb{Z}_2[x]$. Let $K = F[x]/(f(x))$, an extension field*

of $\mathbb{Z}_2$. *Set* $\alpha = x + (f(x))$. $K = \mathbb{Z}_2[\alpha]$. α *is a root of* $f(x)$ *since* $\alpha^3 + \alpha + 1 = 0$. *We have a factorization*

$$x^3 + x + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha + \alpha^2).$$

Thus K *is a splitting field of* $f(x)$ *over* $\mathbb{Z}_2$. $[K : \mathbb{Z}_2] = 3$. K *consists of the 8 elements*

$$K = \{s + t\alpha + u\alpha^2 \mid s, t, u \in \mathbb{Z}_2\}.$$

Definition 0.19. *A field* F *is algebraically closed if* $f(x) \in F[x]$ *and* $deg(f) > 0$ *implies* $f(x)$ *has a root in* F.

By Euclidian division, a field F is algebraically closed if and only if every polynomial $f(x) \in F[x]$ factors into a product of linear factors in $F[x]$.

Definition 0.20. *A field* K *is an algebraic closure of a field* F *if* K *is algebraic over* F *and* K *is algebraically closed.*

The algebraic closure of a field is uniquely determined up to isomorphism.

Theorem 0.21. *Every field has an algebraic closure.*

The idea of the proof of Theorem 0.21 is to successively apply Theorem 0.15 to all polynomials in $F[x]$. This requires some care, as F could have a large cardinality.

By the fundamental theorem of algebra, $\mathbb{C}$ is algebraically closed. As $\mathbb{C}$ is algebraic over $\mathbb{R}$, $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

Define

$$\overline{\mathbb{Q}} = \{u \in \mathbb{C} \mid u \text{ is algebraic over } \mathbb{Q}\}.$$

$\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. As there are transcendental numbers such as π and e, $\overline{\mathbb{Q}}$ is strictly smaller than $\mathbb{C}$.

Since $\mathbb{Q}$ is countable, the polynomials $\mathbb{Q}[x]$ are countable. Since every polynomial of a fixed degree d has at most d roots, we conclude that $\overline{\mathbb{Q}}$ is countable. Since $\mathbb{R}$ is uncountable, $\mathbb{C}$ is uncountable. Thus $\mathbb{C}$ is vastly larger than $\overline{\mathbb{Q}}$.

Definition 0.22. *Suppose that* F *is a subfield of a field* K. $t_1, \ldots, t_r$ *are algebraically independent over* F *if* $f(t_1, \ldots, t_r) \neq 0$ *for every nonzero polynomial* $f(x_1, \ldots, x_r)$ *in the polynomial ring* $F[x_1, \ldots, x_r]$.

It follows from the definition that the surjective ring homomorphism $F[x_1, \ldots, x_r] \to F[t_1, \ldots, t_r]$ defined by $f(x_1, \ldots, x_r) \mapsto f(t_1, \ldots, t_r)$ is an isomorphism if and only if $t_1, \ldots t_r$ are algebraically independent over F.

Lemma 0.23. *Suppose that* r *is a positive integer. Let* L *be a subfield of* $\mathbb{C}$ *which is algebraic over* $\mathbb{Q}$. *Then there exist* $t_1, \ldots, t_r \in \mathbb{C}$ *which are algebraically independent over* L.

Proof. Suppose that there exists a number r such that there do not exist $t_1, \ldots, t_r \in \mathbb{C}$ which are algebraically independent over L. Let r be the smallest number with this property. Set $s = r - 1$. Then there exist elements $t_1, \ldots, t_s$ in $\mathbb{C}$ such that $t_1, \ldots, t_s$ are algebraically independent over L and $\mathbb{C}$ is algebraic over the field $K = L(t_1, \ldots, t_s)$. Thus

$\mathbb{C}$ is an algebraic closure of K. K is countable since L is countable (as $L \subset \overline{\mathbb{Q}}$). Thus the algebraic closure $\mathbb{C}$ of K is countable (by the argument we used to show that $\overline{\mathbb{Q}}$ is countable). This is a contradiction, since $\mathbb{C}$ is uncountable. $\square$

Definition 0.24. *Suppose that F is a subfield of a field K. The F-automorphisms of K is the group*

$$Aut_F K = \{ \text{ field automorphisms } \sigma : K \to K \mid \sigma(a) = a \text{ for } a \in F\}.$$

Suppose that $\eta : F \to K$ is a homomorphism of fields. We have an induced homomorphism of polynomial rings $\overline{\eta} : F[x] \to K[x]$, defined by

$$\overline{\eta}(f(x)) = \eta(a_0) + \eta(a_1)x + \cdots + \eta(a_n)x^n$$

for

$$f(x) = a_0 + a_1x_1 + \cdots + a_nx^n \in F[x],$$

with $a_0, \ldots, a_n \in F$. Denote $\overline{\eta}(f(x))$ by $f^\eta(x)$. We have $(fg)^\eta = f^\eta g^\eta$ for $f, g \in F[x]$.

Theorem 0.25. *Suppose that $\eta : F \to F^*$ is an isomorphism of a field F onto a field F^*. Let K be an extension field of F and K^* be an extension field of F^*. Suppose that $b \in K$ is algebraic over F with minimal polynomial $g(x)$. Then η can be extended to a homomorphism $\zeta : F[b] \to K^*$ if and only if $g^\eta(x)$ has a root in K^*. If $g^\eta(x)$ has a root in K^*, then the number of such extensions is equal to the number of distinct roots of $g^\eta(x)$ in E^*.*

Proof. Suppose that an extension $\zeta : F[b] \to K^*$ exists. Write

$$g(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + x^n$$

with $a_i \in F$. Then

$$\begin{aligned} 0 &= \zeta(0) = \zeta(g(b)) \\ &= \zeta(a_0 + a_1b + a_2b^2 + \cdots + a_{n-1}b^{n-1} + b^n) \\ &= \zeta(a_0) + \zeta(a_1)\zeta(b) + \zeta(a_2)\zeta(b)^2 + \cdots + \zeta(a_{n-1})\zeta(b)^{n-1} + \zeta(b)^n \\ &= \eta(a_0) + \eta(a_1)\zeta(b) + \eta(a_2)\zeta(b)^2 + \cdots + \eta(a_{n-1})\zeta(b)^{n-1} + \zeta(b)^n \\ &= g^\eta(\zeta(b)). \end{aligned}$$

Thus $\zeta(b)$ is a root of g^η in K^*. We further have that ζ is completely determined by $\zeta(b)$.

Conversely, suppose that α is a root of $g^\eta(x)$ in K^*. $g^\eta(x)$ is the minimal polynomial of α over F^* since $g^\eta(x)$ is irreducible in $F^*[x]$ (as $\overline{\eta}$ is an isomorphism). Thus $F^*[\alpha] \cong F^*[x]/(g^\eta(x))$. The isomorphism $\overline{\eta} : F[x] \to F^*[x]$ takes the ideal $(g(x))$ to the ideal $(g^\eta(x))$. Thus we have an induced isomorphism $F[x]/(g(x) \cong F^*[x]/(g^\eta(x))$. Since $F[b] \cong F[x]/(g(x))$, we may compose these isomorphisms to obtain an isomorphism $\zeta : F[b] \cong F^*[\alpha]$ which extends η, and such that $\zeta(b) = \alpha$. $\square$

Corollary 0.26. *Suppose that F is a field, and $f(x)$ is an irreducible polynomial in $F[x]$. Let $K = F[x]/(f(x))$. Then $|Aut_F K|$ is the number of distinct roots of $f(x)$ in K.*

Theorem 0.27. *(Extension Theorem) Suppose that $\eta : F \to F^*$ is an isomorphism of a field F onto a field F^*. Suppose that $f(x) \in F[x]$ is a nonzero polynomial, and let $f^\eta(x)$ be the corresponding polynomial in F^*. Let E be a splitting field of $f(x)$ over F and E^* be a splitting field of $f^\eta(x)$ over F^*. Then η can be extended to an isomorphism of E onto E^*. Moreover, the number of such extensions is less than or equal to $[E : F]$ and it is precisely $[E : F]$ if $f^\eta(x)$ has no multiple roots in E^*.*

Proof. We prove the theorem by induction on $[E : F]$. Let $p(x)$ be an irreducible factor of $f(x)$ in $F[x]$ of degree $d \geq 1$. Then p^η is an irreducible factor of f^η in $F^*[x]$. p^η has $e \leq d = [F[u] : F]$ distinct roots $v_1, \ldots, v_e$ in E^*. Let u be a root of p in E. By Theorem 0.25, there are e distinct extensions of η to a homomorphism from $F[u]$ to E^*, $\eta_i : F[u] \to F^*[v_i]$, where $\eta_i(u) = v_i$. These are all of the extensions of η to a homomorphism $\eta' : F[u] \to E^*$ since $\eta'(u)$ must be a root of p^η in E^*. By induction (replacing F with $F[u]$ and F^* with $F^*[v_i]$), for $1 \leq i \leq e$, there are less than or equal to $[E : F[u]]$ extensions of $\eta_i : F[u] \to E^*$ to a homomorphism $E \to E^*$. Hence there are less than or equal to $[E : F[u]][F[u] : F] = [E : F]$ extensions of η to E, with equality if $f^\eta(x)$ has no multiple roots in E^*.

Such an extension η' of η to E takes a basis of E as a vector space over F to a basis of the image of η' as a vector space over F^*. Thus $[E : F] \leq [E^* : F^*]$. Applying the above proof to $\eta^{-1} : F^* \to F$, we see that $[E^* : F^*] \leq [E : F]$, so that $[E : F] = [E^* : F^*]$. Thus all extensions of η to a homomorphism η' from E to E^* are isomorphisms.

□

Remark 0.28. *We will see in Corollary 0.37, that if F is a field of characteristic zero, then any splitting field E over F of a polynomial in $F[x]$ is the splitting field of a polynomial with no multiple roots.*

Theorem 0.29. *Suppose that K is a splitting field of a nonzero polynomial $f(x) \in F[x]$ of degree n. Then $Aut_F K$ is isomorphic to a subgroup of S_n and thus $|Aut_F K| \leq n!$.*

Proof. Let $u_1, \ldots, u_k$ be the distinct roots of $f(x)$ in K, so that $K = F[u_1, \ldots, u_k]$. Write $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ with $a_i \in F$ and $a_n \neq 0$. Suppose that $\sigma \in \mathrm{Aut}_F K$. Then for $1 \leq i \leq k$,

$$\begin{aligned} 0 &= \sigma(0) \\ &= \sigma(f(u_i)) = \sigma(a_0 + a_1 u_i + a_2 u_i^2 + \cdots + a_n u_i^n) \\ &= \sigma(a_0) + \sigma(a_1)\sigma(u_i) + \sigma(a_2)\sigma(u_i)^2 + \cdots + \sigma(a_n)\sigma(u_i)^n \\ &= a_0 + a_1\sigma(u_i) + a_2\sigma(u_i)^2 + \cdots + a_n\sigma(u_i)^n \\ &= f(\sigma(u_i)). \end{aligned}$$

Thus an element $\sigma \in \mathrm{Aut}_F(K)$ permutes the roots of $f(x)$. Further, since K is generated by $\{u_1, \ldots, u_k\}$ and F, σ fixes all of these roots if and only if σ is the identity map. Thus the map $\Lambda : \mathrm{Aut}_F K \to \mathrm{Sym}(\{u_1, \ldots, u_k\})$ defined by restriction to the set $\{u_1, \ldots, u_k\}$ is a 1-1 group homomorphism. If $k \leq n$, we can include $\{u_1, \ldots, u_k\}$ into a set with n elements to get an inclusion of groups $\mathrm{Sym}(\{u_1, \ldots, u_k\})$ into S_n. □

Example 0.30. *Recall from Example 0.17 that $K = \mathbb{Q}[u, \omega]$ is a splitting field of $x^3 - 2$ over $\mathbb{Q}$, where $u = \sqrt[3]{2}$ is the real cube root of 2 and $\omega = e^{\frac{2\pi\sqrt{-1}}{3}}$. Let $L = \mathbb{Q}[u]$. $[L : \mathbb{Q}] = 3$ but $Aut_{\mathbb{Q}} L = \{id\}$ by Corollary 0.26 since u is the only root of $x^3 - 2$ in L.*

We will determine $Aut_{\mathbb{Q}} K$ by computing its action on the set of roots $\{u, \omega u, \omega u^2\}$ of $x^3 - 2$. Recall from Example 0.17 that $K = L[\omega] \cong L[x]/(x^2 + x + 1)$. Since $\omega, \omega^2 \in K$ are the two roots of $x^2 + x + 1$, it follows from Theorem 0.25 and Corollary 0.26 that $Aut_L K \cong \mathbb{Z}_2$ with generator σ which satisfies $\sigma(\omega) = \omega^2$ and $\sigma(t) = t$ for $t \in L$. Thus

$$\sigma(u) = u, \sigma(u\omega) = u\omega^2, \sigma(u\omega^2) = u\omega.$$

Let $M = \mathbb{Q}[\omega]$.

$$[M[u] : M] = [K : M] = [K : \mathbb{Q}]/[M : \mathbb{Q}] = 3.$$

Thus the minimal polynomial of u over M has degree 3. Since u is a root of the degree 3 monic polynomial $x^3 - 2 \in M[x]$, $x^3 - 2$ is the minimal polynomial of u over M. Thus

$K = M[u] \cong M[x]/(x^3 - 2)$. By Corollary 0.26, $Aut_M K \cong \mathbb{Z}_3$ since $x^3 - 2$ has 3 roots in K. By Theorem 0.25, a generator of $Aut_M K$ is the M-automorphism τ which satisfies $\tau(u) = \omega u$. Thus

$$\tau(u) = \omega u, \tau(u\omega) = u\omega^2, \tau(u\omega^2) = u.$$

We have inclusions of groups $Aut_L K \subset Aut_{\mathbb{Q}} K$ and $Aut_M K \subset Aut_{\mathbb{Q}} K$. Thus $Aut_{\mathbb{Q}} K$ contains an element of order two and an element of order 3. Since $Aut_{\mathbb{Q}} K$ is a subgroup of S_3 by Theorem 0.29, we have that $Aut_{\mathbb{Q}} K \cong S_3$ is generated by σ and τ.

Definition 0.31. *Suppose that F is a field. A nonzero polynomial $f(x) \in F[x]$ of degree n is separable over F if it has n distinct roots in a splitting field N of f over F. If $f(x)$ is not separable over F, it is called inseparable.*

Definition 0.32. *Suppose that F is a field, and $f(x) \in F[x]$ is a polynomial. Write $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_i \in F$. The formal derivative of $f(x)$ is*

$$f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1}.$$

Lemma 0.33. *Suppose that $f, g \in F[x]$. Then*

1. *(f+g)'=f'+g'.*
2. *$(fg)' = fg' + f'g$.*
3. *Suppose that $m \in \mathbb{N}$. Then $(f^m)' = m f^{m-1} f'$.*

Suppose that F is a subfield of a field K, and $f(x), g(x) \in F[x]$ are polynomials. Recall that a greatest common divisor of $f(x)$ and $g(x)$ in $F[x]$ is a greatest common divisor of $f(x)$ and $g(x)$ in $K[x]$. To prove this, observe that a greatest common divisor of $f(x)$ and $g(x)$ in $F[x]$ is a generator d of the principal ideal generated by f and g in $F[x]$. Thus d is also a generator of the ideal generated by f and g in $K[x]$, and thus d is a greatest common divisor of f and g in $K[x]$ also.

Theorem 0.34. *Suppose that F is a field and $f(x) \in F[x]$ is a nonzero polynomial. Then $f(x)$ is separable over F if and only if 1 is a greatest common divisor of f and f'.*

Proof. Let N be a splitting field of f over F. Let $u_1, \ldots, u_k$ be the distinct roots of $f(x)$ in N. Then there exist positive integers $e_1, \ldots, e_k$ and a nonzero $c \in F$ such that

$$f(x) = c(x - u_1)^{e_1}(x - u_2)^{e_2} \cdots (x - u_k)^{e_k}.$$

We have

$$f'(x) = c\left(e_1(x - u_1)^{e_1 - 1}(x - u_2)^{e_2} \cdots (x - u_k)^{e_k} + (x - u_1)^{e_1}\left[(x - u_2)^{e_2} \cdots (x - u_k)^{e_k}\right]'\right).$$

Thus $(x - u_1)$ divides $f'(x)$ in $N[x]$ if and only if $e_1 > 1$. The same argument applied to other factors of $f(x)$ shows that $x - u_i$ divides $f'(x)$ in $N[x]$ if and only if $e_i > 1$. Since the only irreducible factors of $f(x)$ in $N[x]$ are $x - u_i$, $1 \leq i \leq k$, we have that 1 is a greatest common divisor of f and f' if and only if $e_i = 1$ for $1 \leq i \leq k$. □

Corollary 0.35. *Suppose that F is a field and $f(x) \in F[x]$ is an irreducible polynomial. Then $f(x)$ is separable unless its formal derivative is zero.*

Proof. Suppose that $f(x)$ is not separable. Since 1 is not a greatest common divisor of f and f', and $f(x)$ is irreducible, we have that $f(x)$ divides $f'(x)$. Thus $f' = 0$ since $\deg(f') < \deg(f)$. □

Corollary 0.36. *Suppose that F is a field of characteristic zero. If $f(x) \in F[x]$ is an irreducible polynomial, then $f(x)$ is separable.*

Proof. Since F has characteristic zero, and $f(x)$ has positive degree, $f'(x) \neq 0$. □

Corollary 0.37. *If K is a splitting field over a field F of characteristic zero of a polynomial $f(x) \in F[x]$, then K is the splitting field of a separable polynomial over F.*

Proof. Let g be the product of the distinct irreducible factors of f in $F[x]$. Then K is the splitting field of $g(x)$. The irreducible factors of $g(x)$ are separable by Corollary 0.36. Since the irreducible factors of g must be relatively prime (in $F[x]$ and $K[x]$), they have no common roots. Thus g is separable □

Example 0.38. *Let $F = \mathbb{Z}_p(t)$ where p is a prime number and t is an indeterminate. Let $f(x) = x^p - t \in F[x]$. $f(x)$ is irreducible but $f(x)$ is not separable over F, as $f(x) = (x - \sqrt[p]{t})^p$. A splitting field of f over F is $K = F[\sqrt[p]{t}]$. $[K : F] = p$, but $Aut_F K = \{id\}$.*

Theorem 0.39. *Suppose that N is the splitting field of a separable polynomial $f(x) \in F[x]$. Then $|Aut_F N| = [N : F]$.*

Proof. By the Extension Theorem (Theorem 0.27), the identity automorphism of F extends to $[N : F]$ distinct automorphisms of N, since $f(x)$ has no multiple roots. □

Definition 0.40. *Let G be a finite group of automorphisms of a field K. Define the fixed field K^G of G by*

$$K^G = \{a \in K \mid \sigma(a) = a \text{ for all } a \in K\}.$$

The fact that K^G is a field follows from the facts that K is a field and G is a group of automorphisms. The fixed field of $\mathrm{Aut}_F K$ necessarily contains F.

Definition 0.41. *Suppose that F is a subfield of a field K and K is finite over F (that is $[K : F] < \infty$). We say that K is Galois over F (or K/F is Galois) if F is the fixed field of $Aut_F K$.*

If F is a subfield of a field K and L is the fixed field of $\mathrm{Aut}_F K$, then K is Galois over L.

Theorem 0.42. *Suppose that F is a subfield of a field N. Then N is the splitting field of a separable polynomial $f(x) \in F[x]$ if and only if N/F is Galois.*

Proof. First suppose that N is a splitting field of a separable polynomial $f(x) \in F[x]$. Let K be the fixed field of $\mathrm{Aut}_F N$. Then N is a splitting field of F over K and $f(x)$ is separable over K also. By applying Theorem 0.39 to both subfields F and K of N, we have

$$|\mathrm{Aut}_F N| = [N : F] = [N : K][K : F] = |\mathrm{Aut}_K N|[K : F].$$

Since $\mathrm{Aut}_F N = \mathrm{Aut}_K N$, we have $[K : F] = 1$ and thus $K = F$, since 1 is then a basis of K as a vector space over F.

Now suppose that N is Galois over F. Let $G = \mathrm{Aut}_F N$. $N = F[u_1, \ldots, u_k]$ for some $u_i \in N$. For $1 \leq i \leq k$, let $a_{i,1}, \ldots, a_{i,\lambda_i}$ be the distinct elements of the set

$$S_i = \{\sigma(u_i) \mid \sigma \in G\}.$$

Any two of these sets S_i are either disjoint or equal. After reindexing, we may assume that the first n sets $S_1, \ldots, S_n$ are pairwise disjoint, and every S_i for $1 \leq i \leq k$ is one of

these sets. We have that N is generated over F be the sets $S_1, \ldots, S_n$. Let

$$f(x) = \prod_{i=1}^{n} \prod_{j=1}^{\lambda_i} (x - a_{i,j}) \in N[x].$$

$f(x)$ is separable, and

$$f^{\eta}(x) = \prod_{i=1}^{n} \prod_{j=1}^{\lambda_i} (x - \eta(a_{i,j})) = f(x)$$

for $\eta \in G$, since η permutes the $a_{ij} \in S_i$. Thus η fixes the coefficients of $f(x)$, and it follows that $f(x) \in F[x]$, since F is the fixed field of G. Thus N is a splitting field of f over F.

□

Example 0.43. *The splitting field K of an irreducible (and hence separable) quadratic polynomial $f(x) \in \mathbb{Q}[x]$ (Example 0.16) is Galois with $Aut_{\mathbb{Q}}K \cong \mathbb{Z}_2$.*

Example 0.44. *Let $u = \sqrt[3]{2}$ be the real cube root of 2, and let $\omega = e^{\frac{2\pi\sqrt{-1}}{3}}$, a cube root of unity. Let K be the splitting field of $x^3 - 2$ over $\mathbb{Q}$ constructed in Examples 0.17 and 0.30. $f = x^3 - 2$ is separable ($f' = 3x^2 \neq 0$). Thus K is Galois over $\mathbb{Q}$. We showed that $Aut_{\mathbb{Q}}K \cong S_3$. The intermediate field $L = \mathbb{Q}[u]$ is not Galois over $\mathbb{Q}$, as the only root of $x^3 - 2$ in L is u. We computed that $Aut_{\mathbb{Q}}L = \{id\}$, so $1 = |Aut_{\mathbb{Q}}L| < [L : \mathbb{Q}] = 3$. However, K is Galois over L with $Aut_L K \cong \mathbb{Z}_2$. Let $M = \mathbb{Q}[\omega]$. M is a splitting field for the separable polynomial $g = x^2 + x + 1$ over $\mathbb{Q}$ ($g' = 2x \neq 0$) so M is Galois over $\mathbb{Q}$. We have $Aut_{\mathbb{Q}}M \cong \mathbb{Z}_2$. K is Galois over M with $Aut_M K \cong \mathbb{Z}_3$.*

Theorem 0.45. *Let F be a field of characteristic zero, and r be a positive integer. Then there exists an extension field K of F and a splitting field N of F such that $Aut_K N \cong S_r$.*

Proof. Let $t_1, \ldots, t_r$ be algebraically independent over F. Expand the product $f(x) = (x-t_1)(x-t_2)\cdots(x-t_r)$ as $f(x) = x^r - P_1 x^{r-1} + \cdots + (-1)^r P_r$ with each $P_i \in F[t_1, \ldots, t_r]$. $P_1, \ldots, P_r$ are called the elementary symmetric functions of $t_1, \ldots, t_r$. For every $\sigma \in S_r$, we have (by Theorem 0.1) an F-automorphism $T_\sigma : F[t_1, \ldots, t_r] \cong F[t_1, \ldots, t_r]$ defined by $T_\sigma(t_i) = t_{\sigma(i)}$ for $1 \leq i \leq r$. T_σ induces an F-automorphism of $N = F(t_1, \ldots, t_r)$. Set $K = F(P_1, \ldots, P_r)$. We have that $f(x) \in K[x]$, and N is a splitting field of $f(x)$. We have $T_\sigma \in \mathrm{Aut}_K N$ for all $\sigma \in S_r$. Thus $\mathrm{Aut}_K N$ contains a subgroup isomorphic to S_r. Since $f(x)$ has degree r, $\mathrm{Aut}_K N$ is then isomorphic to S_r by Theorem 0.29. □

Definition 0.46. *A finite group G is called solvable if it contains a chain of subgroups*

$$\{0\} = G_s \subset G_{s-1} \subset \cdots \subset G_2 \subset G_1 = G$$

such that G_{i+1} is a normal subgroup of G_i for all i and G_i/G_{i+1} is abelian for all i.

Lemma 0.47. *Let G be a group and H a normal subgroup. Then G is solvable if and only if H and G/H are solvable.*

This is proven in Theorem I.3.2 [1].

Theorem 0.48. *The symmetric group S_n is not solvable if $n \geq 5$.*

This is proven in Theorem I.5.4 [1].

Definition 0.49. *Suppose that F is a subfield of a field K. K is a radical extension of F if there exists a sequence of subfields*

$$F = K_0 \subset K_1 = F[u_1] \subset K_2 = K_1[u_2] \subset \cdots \subset K_n = K_{n-1}[u_n] = K \tag{4}$$

and for $1 \leq i \leq n$ there exist positive integers r_i such that $a_i = u_i^{r_i} \in K_{i-1}$.

There are examples of field extensions $F \subset E \subset K$ such that K is Galois over E and E is Galois over F but K is not Galois over F (see Exercise 15).

Lemma 0.50. *Suppose that F is a field of characteristic zero and K is a radical extension of F. Then there exists a radical extension N of F which is Galois over F and contains K.*

Proof. Suppose that K is generated by $v_1, \ldots, v_r$ over F. Let $g_i(x)$ be the minimal polynomial of v_i over F, and let L be a splitting field of $\prod_{i=1}^r g_i$ over F which contains K (L exists by Theorem 0.15). L is Galois over F by Corollary 0.37 and Theorem 0.42. Let $G = \mathrm{Aut}_F L$. Write K as a tower of fields of (4). Let

$$f(x) = \prod_{i=1}^{n} \prod_{\sigma \in G} (x - \sigma(u_i)).$$

We have that $f^\tau = f$ for $\tau \in G$, since τ permutes the roots of f, so the coefficents of $f(x)$ are in the fixed field F of G. Thus $f(x) \in F[x]$. Index G as $G = \{\sigma_1, \ldots, \sigma_s\}$, where $s = |G| = [L : F]$. Define

$$E_{ij} = \begin{cases} E_{0,0} & \text{if } i = j = 0, \\ E_{i-1,s-1}[\sigma_s(u_i)] & \text{if } i > 0 \text{ and } j = 0, \\ E_{i,j-1}[\sigma_j(u_{i+1})] & \text{if } 1 \leq j \leq s-1. \end{cases}$$

Let $N = E_{n,0}$. We have a tower of fields

$$F = E_{0,0} \to E_{0,1} \to \cdots E_{0,s-1} \to E_{1,0} \to \cdots \to E_{n-1,s-1} \to E_{n,0} = N. \tag{5}$$

Further,

$$\sigma_j(u_{i+1})^{r_{i+1}} = \sigma_j(u_{i+1}^{r_{i+1}}) \in \sigma_j(K_i) \subset E_{i,0} \subset E_{i,j-1}$$

for all i and j. Thus (5) is a radical extension. Since N is a splitting field of $f(x)$ over F, and F has characteristic zero, N is Galois over F by Theorem 0.42. By our construction, N contains K. □

Definition 0.51. *Suppose that E is a splitting field of a separable polynomial $f(x) \in F[x]$. E is solvable by radicals over F (and $f(x) = 0$ is solvable by radicals over F) if E is a subfield of a radical extension of F.*

Suppose that F is a field and $f(x) \in F[x]$ is a polynomial. We would like to find a *rational formula for constructing the roots* of $f(x)$; that is, we would like to break up the solution of $f(x) = 0$ into a sequence of operations on numbers already determined, each individual operation being addition, multiplication, subtraction or division or the extraction of an n-th root.

An example of a rational formula for contructing roots is the quadratic formula. There are similar formulas for solving cubic and quartic equations (given at the beginning of these notes). The impossibility of finding such a formula for equations of degree ≥ 5 was found in the 19th century (by Abel, Ruffini and Galois). We will now prove this result.

If there is a rational formula for constructing the roots of $f(x) \in F[x]$, then the roots of $f(x)$ are contained in a radical extension K of F; that is, $f(x)$ is solvable by radicals over F.

The formulas for solving cubics and quartics $f(x)$ may lead to the construction of a radical extension K of F which properly contains a splitting field E of $f(x)$. We will prove the impossibility of solving the general polynomial of degree ≥ 5. The proof is simpler if we assume that our field F already contains all roots of unity, so we make this assumption.

Lemma 0.52. *Suppose that F is a subfield of $\mathbb{C}$ which contains all roots of unity and $K = F[u]$ is a subfield of $\mathbb{C}$ where $a = u^r \in F$. Then*

1. *K is a splitting field of $x^r - a$ over F (so that K is Galois over F by Theorem 0.42).*
2. *$Aut_F K$ is isomorphic to $\mathbb{Z}_s$, where s divides r.*

Proof. The roots of $x^r - a$ are $\tau^i u$ for $0 \leq i \leq r-1$, where $\tau = e^{\frac{2\pi\sqrt{-1}}{r}} \in F$. Thus $\tau^i u \in K$ for all i, so that K is a splitting field of $x^r - a$ over F.

Let s be the smallest positive integer such that $u^s \in F$. Write $r = as + b$ with $0 \leq b < s$. $u^b = \frac{u^r}{(u^s)^a} \in F$ implies $b = 0$. Hence s divides r. let $\alpha = u^s \in F$. Let $f(x) = x^s - \alpha \in F[x]$. Let $\omega = e^{\frac{2\pi\sqrt{-1}}{s}} \in F$. Suppose that a monic nonconstant polynomial $g(x) \in F[x]$ divides $f(x)$. Let $n \leq s$ be the degree of $g(x)$. Then the constant term of $g(x)$ is $\omega^i u^n$ for some integer i, so that $u^n \in F$. Thus $n = s$ and $g(x) = f(s)$, so that $f(x)$ is irreducible in $F[x]$. Since $f(u) = 0$, $f(x)$ is the minimal polynomial of u over F. By Theorem 0.25, the F-automorphisms of K are maps $\Phi_i : K \to K$ for $1 \leq i \leq s-1$, which are defined by the two conditions $\Phi_i(u) = \omega^i u$ and $\Phi_i(\gamma) = \gamma$ for $\gamma \in F$. For a given i, we have $\Phi_i(u) = \omega^i u = \Phi_1^i(u)$, and $\Phi_i(\gamma) = \Phi_1^i(\gamma) = \gamma$ for $\gamma \in F$. Thus $\Phi_i = \Phi_1^i$, and $\mathrm{Aut}_F K \cong \mathbb{Z}_s$ with generator Φ_1. □

Lemma 0.53. *Suppose that F is a subfield of $\mathbb{C}$ which contains all roots of unity and K is a radical Galois extension of F which is contained in $\mathbb{C}$. Then $Aut_F K$ is solvable.*

Proof. We have a sequence of fields

$$F = K_0 \subset K_1 = F[u_1] \subset K_2 = K_1[u_2] \subset \cdots \subset K_n = K_{n-1}[u_n] = K \tag{6}$$

and there exist positive integers r_i such that $a_i = u_i^{r_i} \in K_{i-1}$, with $u_i \notin K_{i-1}$.

We prove that $\mathrm{Aut}_F K$ is solvable by induction on $[K : F]$. Given $\sigma \in \mathrm{Aut}_F K$, $\sigma(u_1)$ is a root of $x^{r_1} - a_1 \in F[x]$. Thus $\sigma(u_1) = \tau u_1$ where τ is an r_1-th root of unity. It follows that $\sigma : K_1 \to K_1$. So restriction to K_1 gives us a homomorphism $\Lambda : \mathrm{Aut}_F K \to \mathrm{Aut}_F K_1$. Λ is a surjection since the Extension Theorem (Theorem 0.27) shows that any $\sigma \in \mathrm{Aut}_F K_1$ extends to $\mathrm{Aut}_F K$. $\mathrm{Aut}_F K_1 \cong \mathbb{Z}_s$ for some s by Lemma 0.52. The kernel of Λ is

$$\mathrm{Kernel}(\Lambda) = \{\sigma \in \mathrm{Aut}_F K : \text{ the restriction } \sigma | K_1 = \mathrm{id}\} = \mathrm{Aut}_{K_1} K.$$

By induction on $[K : F]$, we have that $\mathrm{Aut}_{K_1} K$ is solvable, since K is a radical Galois extension of K_1, and

$$[K : K_1] = [K : F]/[K_1 : F] < [K : F].$$

Since the kernel and image of of Λ are solvable, $\mathrm{Aut}_F K$ is solvable by Lemma 0.47. □

Theorem 0.54. *Suppose that F is a subfield of $\mathbb{C}$ which contains all roots of unity and E is a subfield of $\mathbb{C}$ which is a splitting field over F such that E is solvable by radicals over F. Then $Aut_F E$ is solvable.*

Proof. By Lemma 0.50, E is a subfield of a radical Galois extension K of F.

K is a splitting field over E since K is a splitting field over F. Restriction to E gives a group homomorphism $\mathrm{Aut}_F K \to \mathrm{Aut}_F E$ since E is a splitting field over F. Further, $\mathrm{Aut}_F K \to \mathrm{Aut}_F E$ is onto by the Extension Theorem (Theorem 0.27). By Lemmas 0.53 and 0.47, $\mathrm{Aut}_F E$ is solvable.

□

Theorem 0.55. *For every integer $r \geq 5$ there exists a subfield F of $\mathbb{C}$ and a polynomial $f(x) \in F[x]$ of degree r which is not solvable by radicals over F.*

Proof. Let L be a subfield of $\overline{\mathbb{Q}}$ which contains all roots of unity. By Lemma 0.23, there exist $t_1, \ldots, t_r \in \mathbb{C}$ which are algebraically independent over L. Let $F = L(P_1, \ldots, P_r)$ where P_i are the elementary symmetric functions of the t_i. Let $K = F(t_1, \ldots, t_r)$. K is a splitting field of

$$f(x) = x^r - P_1 x^{r-1} + \cdots + (-1)^r P_r = (x - t_1)(x - t_2) \cdots (x - t_r)$$

over F. $\mathrm{Aut}_F K = S_r$ by Theorem 0.45. S_r is not solvable for $r \geq 5$ by Theorem 0.48, so $f(x)$ is not solvable by radicals over F by Theorem 0.54 □

We end by stating a few more results, which will be useful in the exercises.

Definition 0.56. *Suppose that K is an algebraic extension of a field F. K is a normal extension of F if every irreducible polynomial in $F[x]$ which has a root in K is a product of linear factors in $K[x]$.*

Theorem 0.57. *Suppose that K is a splitting field of a polynomial $f(x) \in F[x]$. Then K is a normal extension of F.*

This is proven in Theorem 33 [1].

Theorem 0.58. *Let G be a finite group of automorphisms of a field K. Then*

$$[K : K^G] \leq |G|. \tag{7}$$

Proof. Let $F = K^G$. The fact that F is a field follows from the facts that K is a field and G is a group of automorphisms. Let $n = |G|$. Index G as $G = \{\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n\}$. Suppose that $u_1, \ldots, u_m \in K$ with $m > n$. We will show that $u_1, \ldots, u_m$ are linearly independent over F. Since $u_1, \ldots, u_m \in F$ are arbitrary, it will follow that $[K : F] \leq n$, which establishes (7).

The homogeneous system of equations

$$\sum_{j=1}^{m} \sigma_i(u_j) x_j = 0, \;\; 1 \leq i \leq n \tag{8}$$

in the n unknowns $x_1, \ldots, x_m$ has a nontrivial solution in K^m since $m > n$.

Choose a nontrivial solution $(b_1, \ldots, b_m)$ to (8) with the least number of nonzero b_i. After possibly reordering the b_i, we may assume that $b_1 \neq 0$. Since $b_1^{-1}(b_1, \ldots, b_m)$ is also a solution, we may assume that $b_1 = 1$. We will next establish that every b_j is in F. This

will prove the linear dependence of $u_1, \ldots, u_n$ over F since from the first equation of (8) we have the dependence relation

$$\sum_{j=1}^{m} u_j b_j = 0.$$

Suppose some $b_j \notin F$. We will derive a contradiction. After possibly reindexing the b_i, we may assume that $b_2 \notin F$. Since F is the fixed field of G, there exists $\sigma_k \in G$ such that $\sigma_k(b_2) \neq b_2$. Apply σ_k to the system of equations

$$\sum_{j=1}^{m} \sigma_i(u_j) b_j = 0, \;\; 1 \leq i \leq n$$

to get

$$\sum_{j=1}^{m} (\sigma_k \sigma_i)(u_j) \sigma_k(b_j) = 0, \;\; 1 \leq i \leq n.$$

Since $(\sigma_k\sigma_1, \ldots, \sigma_k\sigma_n)$ is a permutation of $(\sigma_1, \ldots, \sigma_n)$, we have the system

$$\sum_{j=1}^{m} \sigma_i(u_j) \sigma_k(b_j) = 0, \;\; 1 \leq i \leq n.$$

Thus $(1, \sigma_k(b_2), \ldots, \sigma_k(b_m))$ is also a solution to (8). Subtracting this from the solution $(1, b_2, \ldots, b_m)$, we obtain the solution $(0, b_2 - \sigma_k(b_2), \ldots, b_m - \sigma_k(b_m))$ which is nontrivial since $b_2 - \sigma_k(b_2) \neq 0$. This solution has fewer nonzero entries than $(b_1, b_2, \ldots, b_m)$, in contradiction to our choice of $(b_1, \ldots, b_m)$. Thus all b_i are in F, from which we obtain $[K : F] \leq |G|$. □

Theorem 0.58 is a major ingredient in the proof of the following "Fundamental Theorem of Galois Theory".

Theorem 0.59. *Suppose that K is a finite field extension of a field F such that K is Galois over F. Let $G = Aut_F K$. Then the function $H \mapsto K^H$ is a bijective map from the set of subgroups of G to the set of intermediate fields E between F and K. The inverse function is $E \mapsto Aut_E K$. The correspondence has the following properties.*

1. *If E is an intermediate field between F and K then $[K : E] = |Aut_E K|$ and $[E : F] = [G : Aut_E K]$.*
2. *A subgroup H of G is a normal subgroup of G if and only if K^H is a normal field extension of F. In this case, $Aut_F K^H \cong G/H$.*

This theorem is proven in Chapter VI, Section 1 on "Galois Theory" in [1].

Exercises

1. Prove Theorem 0.1.
2. Prove Lemma 0.7.
3. Prove Lemma 0.9.
4. Prove Lemma 0.12
5. Prove Corollary 0.26. Be sure to establish that any homomorphism from K to K you construct is onto, so that it is actually an isomorphism.
6. Suppose that $f(x) \in \mathbb{R}[x]$ is a polynomial. Show that the nonreal roots of $f(x)$ are of an even number, consisting of pairs of a complex number and its complex conjugate.

7. Let K be a splitting field of $f(x) = x^4 - 2x^2 + 9$ over $\mathbb{Q}$.
   a. Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.
   b. Compute the index $[K : \mathbb{Q}]$.
   c. Compute the order of $\mathrm{Aut}_{\mathbb{Q}}K$.
   d. Compute the group $\mathrm{Aut}_{\mathbb{Q}}K$. If it is isomorphic to a group you know, identify the group.
8. Let K be a splitting field of $f(x) = x^5 - 6x + 3$ over $\mathbb{Q}$.
   a. Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.
   b. Compute the index $[K : \mathbb{Q}]$.
   c. Compute the order of $\mathrm{Aut}_{\mathbb{Q}}K$.
   d. Compute the group $\mathrm{Aut}_{\mathbb{Q}}K$. If it is isomorphic to a group you know, identify the group.

Some hints for Problem 8: Use calculus to show that $f(x)$ has exactly 3 real roots. You may use (without proof) the following Sylow Theorem.

Let G be a finite group, H a subgroup, p a prime number. H is called a *Sylow Subgroup* of G if $|H| = p^n$ and p^n is the largest power of p dividing $|G|$.

Theorem 0.60. *(Theorem I.6.2* [1]*) Let G be a finite group and p a prime number dividing the order of G. Then there exists a p-Sylow subgroup of G.*

9. Suppose that F is a field and u is algebraic over F, where the degree of the minimal polynomial of u over F is odd. Show that $F[u] = F[u^2]$.
10. Suppose that G is a finite group. Show that there exists a field F and a polynomial $f(x) \in F[x]$ which is separable over F such that $G \cong \mathrm{Aut}_F K$ where K is a splitting field of $f(x)$ over F.
11. Prove the following lemma:

    Lemma 0.61. *Suppose that F is a subfield of $\mathbb{C}$, r is a positive integer, and $\omega = e^{\frac{2\pi\sqrt{-1}}{r}}$. Let $K = F[\omega]$. Then K is Galois over F and $Aut_F K$ is Abelian.*

12. Use Lemma 0.61 to prove the following theorem:

    Theorem 0.62. *Suppose that F is a subfield of $\mathbb{C}$ and E is a subfield of $\mathbb{C}$ which is a splitting field over F such that E is solvable by radicals over F. Then $Aut_F E$ is solvable.*

13. Use Theorem 0.62 to give an example of a polynomial which is not solvable by radicals over $\mathbb{Q}$.
14. Prove Theorem 0.57.
15. Give an example of finite field extensions $F \subset E \subset K$ such that K is Galois over E and E is Galois over F, but K is not Galois over F. Hint: Use the Fundamental Theorem of Galois Theory.
16. Deduce from the "Fundamental Theorem of Algebra" that the irreducible polynomials in the polynomial ring $\mathbb{R}[x]$ are the linear polynomials and the quadratic polyomials with negative discriminant.
17. Suppose that F is a field of characteristic zero and K is a finite field extension. Show that there are only finitely many intermediate field L between F and K.

References

[1] Serge Lang, *Algebra, revised third edition*, Springer-Verlag, New York, Berlin, Heidelberg (2002).