GALOIS THEORY

Notes by L.H. Walling and T.D. Wooley

The notes are organised into the following sections.

References: Besides the course notes (as posted on the instructors' websites), the following are recommended.

(1) "Algebra" by P. Grillet (available electronically through the UoB library), and
(2) "A Course in Galois Theory" by D.J.H. Garling.

0. Introduction

Recall that with R, R' commutative rings with unity (where "unity" means a multiplicative identity), $\varphi : R \to R'$ is a homomorphism if, for all $x, y \in R$,

(1) $\varphi(x+y) = \varphi(x) + \varphi(y)$;
(2) $\varphi(xy) = \varphi(x)\varphi(y)$;
(3) $\varphi(1) = 1$.

With K, L fields, we say L is an extension of K if there is a homomorphism $\varphi : K \to L$. Suppose such φ exists. We know $\ker \varphi$ is an ideal of K. As K is a field, its only ideals are $\{0\}$ and K. We know that $\varphi(1) = 1$ and $1 \neq 0$, so $1 \notin \ker \varphi$. Hence $\ker \varphi \neq K$, so $\ker \varphi = \{0\}$, meaning that φ is injective. So when $L : K$ is a field extension, L contains an isomorphic image of K.

Suppose K is a field, and f is a polynomial in the ring $K[t_1]$ with $\deg f = n \geq 1$. The polynomial ring $K[t_1]$ is a unique factorisation domain, and since f is not 0 or a unit, f factors (essentially uniquely) as a product of

irreducible elements of $K[t_1]$. Let $g_1 \in K[t_1]$ be an irreducible factor of f. Recall that the ideal generated by g_1 is

$$(g_1) = \{g_1 h : \ h \in K[t_1] \ \},$$

and since g_1 is irreducible, $I_1 = (g_1)$ is a maximal ideal. Hence $K_1 = K[t_1]/I_1$ is a field, and $\varphi_1 : K \to K_1$ defined by $\varphi_1(c) = c + I_1$ is an injective homomorphism. We can naturally extend φ_1 to a homomorphism $\varphi_1 : K[t_1] \to K_1[t_2]$, defining $\varphi_1 : K[t_1] \to K_1[t_2]$ by

$$\varphi_1 \left(\sum_{i=0}^{d} c_i t_1^i \right) = \sum_{i=0}^{d} \overline{c}_i t_2^i$$

where $\overline{c} = c + I_1 = \varphi_1(c)$. (So we are slightly abusing notation by calling this extended homomorphism φ_1.) Write

$$g_1 = a_0 + a_1 t_1 + \cdots + a_d t_1^d$$

where $a_0, a_1, \ldots, a_d \in K$. Let $\alpha_1 = t_1 + I_1$. Then with $(\varphi_1(g_1))(\alpha_1)$ denoting the polynomial $\varphi_1(g_1)$ evaluated at α_1, we have that

$$\begin{aligned}
(\varphi_1(g_1))(\alpha_1) &= \sum_{j=0}^{d} \overline{a}_j \alpha_1^j \\
&= \sum_{j=0}^{d} (a_j + I_1)(t_1 + I_1)^j \\
&= \sum_{j=0}^{d} (a_j t_1^j + I_1) \\
&= \left(\sum_{j=0}^{d} a_j t_1^j \right) + I_1 \\
&= g_1 + I_1 \\
&= 0 + I_1
\end{aligned}$$

since $g_1 = \sum_{j=0}^{d} a_j t^j \in I_1$. So in K_1, α_1 is a root of $\varphi_1(g_1)$. Since g_1 divides f, we have that $\varphi_1(g_1)$ divides $\varphi_1(f)$, so α_1 is a root of $\varphi_1(f)$. Hence in $K_1[t_2]$, $\varphi_1(f) = (t_2 - \alpha_1)h_1$ where $h_1 \in K_1[t_2]$ with $\deg h_1 = (\deg f) - 1$.

Repeating the above argument (finitely many times), we construct a sequence of homomorphisms:

$$K \xrightarrow{\varphi_1} K[t_1]/I_1 = K_1 \xrightarrow{\varphi_2} K_1[t_2]/I_2 = K_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_m} K_{m-1}[t_m]/I_m = L$$

where each I_j is a maximal ideal of $K_{j-1}[t_j]$, K_j contains (at least) j roots of $\varphi_j \circ \cdots \circ \varphi_2 \circ \varphi_1(f)$, and with $\varphi = \varphi_m \circ \cdots \circ \varphi_2 \circ \varphi_1$, $t = t_{m+1}$, we have

$$\varphi(f) = \lambda(t - \beta_1)(t - \beta_2) \cdots (t - \beta_n)$$

where $\lambda, \beta_1, \ldots, \beta_n \in L$. (Actually, $\lambda \in \varphi(K)$ is the image under φ of the leading coefficient of f.) Also, $\varphi : K \to L$ is a homomorphism, so $L : K$ is a field extension. (Note that we could prove this more formally using induction, with an induction step to show that for K, f as above and $\ell < n$, if there is a field extension E of K containing ℓ roots of (the image of) f,

then there is a field extension F of K containing $\ell + 1$ roots of (the image of) f.)

Given $L : K$ a field extension with the homomorphism φ, we can identify K with its isomorphic image in L (meaning that for each $c \in K$, we identify c with $\varphi(c)$), and thus we can assume $K \subseteq L$.

Suppose $L : K$ is a field extension, and consider the automorphisms of L that leave K pointwise fixed. These automorphisms form a group under composition, called the Galois group of $L : K$, and denoted $Gal(L : K)$. For a finite extension $L : K$, we say $L : K$ is a Galois extension if $L = K(\alpha_1, \ldots, \alpha_n)$ where $f \in K[t]$ and $f = \lambda(t - \alpha_1) \cdots (t - \alpha_n)$ with $\lambda \in K$, and $\alpha_1, \ldots, \alpha_n$ are **distinct** elements of L. (Recall that $L = K(\alpha_1, \ldots, \alpha_n)$ is the smallest field containing K and $\alpha_1, \ldots, \alpha_n$.) When $L : K$ is a Galois extension, we have $[L : K] = |Gal(L : K)|$, and the Fundamental Theorem of Galois Theory gives us a one-to-one correspondence between all subgroups of $Gal(L : K)$ and all fields F with $K \subseteq F \subseteq L$: For H a subgroup of $Gal(L : K)$, let

$$F = \{\beta \in L : \ \forall \sigma \in H, \ \sigma(\beta) = \beta \ \}.$$

Then F is a subfield of L containing K, and is denoted by L^H. On the other hand, suppose we have a field F with $K \subseteq F \subseteq L$. Let

$$H = \{\sigma \in Gal(L : K) : \ \forall \beta \in F, \ \sigma(\beta) = \beta \ \}.$$

Then H is a subgroup of $Gal(L : K)$, and in fact, $H = Gal(L : F)$. Further, for H a subgroup of $Gal(L : K)$, we have $H = Gal(L : L^H)$, and for a field F with $K \subseteq F \subseteq L$, $F = L^{Gal(L:F)}$. So the maps $H \mapsto L^H$ and $F \mapsto Gal(L : F)$ are inverses of each other. Finally, H is a normal subgroup of $Gal(L : K)$ if and only if $L^H : K$ is a Galois extension; in the case that H is a normal subgroup of $Gal(L : K)$, $Gal(L^H : K) \simeq Gal(L : K)/H$.

Zorn's Lemma and existence of maximal ideals.

In this course, we assume Zorn's Lemma (stated below). Note that Zorn's Lemma is equivalent to the Axiom of Choice, which is controversial among some mathematicians. However, most mathematicians assume the Axion of Choice, and hence assume Zorn's Lemma.

Zorn's Lemma: Suppose X is a nonempty, partially ordered set with $\leq$ denoting the partial ordering. A chain C in X is a collection of elements $\{a_i\}_{i \in I}$ of X so that for every $i, j \in I$, either $a_i \leq a_j$ or $a_j \leq a_i$. Suppose that every nonempty chain C in X has an upper bound in X; then X has a maximal element m, meaning that if $b \in X$ with $m \leq b$, then $b = m$. (Note that if we have a totally ordered set, a maximal element of the set is the same as a maximum of the set.)

Proposition 0.1. *Any proper ideal A of a commutative ring R is contained in a maximal ideal.*

Proof. Let $\mathcal{S}$ be the set of all proper ideals of R that contain A; so $\subseteq$ gives us a partial ordering on $\mathcal{S}$. Clearly $A \in \mathcal{S}$, so $\mathcal{S} \neq \emptyset$. Suppose $\{J_i\} i \in \mathcal{I}$ is a (nonempty) chain in $\mathcal{S}$. Set $J = \cup_{i \in \mathcal{I}} J_i$. Then $1 \notin J$, since $\forall i \in \mathcal{I}$, $1 \notin J_i$. So $J \neq R$. It is easy to check that J is an ideal of R. Thus $J \in \mathcal{S}$, and $\forall i \in \mathcal{I}$, $J_i \subseteq J$. Hence by Zorn's Lemma, $\mathcal{S}$ contains a maximal element B. So B is an ideal with $A \subseteq B \subsetneq R$. Suppose C is an ideal so that

$B \subsetneq C \subseteq R$. Thus either C is in $\mathcal{S}$, contradicting that B is maximal in $\mathcal{S}$, or $C = R$. Hence B is a maximal ideal. □

1. Field extensions and algebraic elements: an enhanced review

As discussed in the introduction [and proved in Algebra 2], we have the following.

Proposition 1.1. *Suppose K, L are fields and $\varphi : K \to L$ is a homomorphism. Then φ is injective.*

Definition. Suppose K, L are fields and $\varphi : K \to L$ is a homomorphism (and thus φ is necessarily an embedding, i.e. an injective homomorphism). Then we say L is a field extension of K (relative to the embedding φ), or equivalently, that $L : K$ is a field extension. When K, L are fields with $K \subseteq L$, we assume $\varphi : K \to L$ is the identity map on K.

Proposition 1.2. *Suppose $L : K$ is a field extension. Then L is a vector space over K.*

Proof. [Proved in Algebra 2] Since $L : K$ is a field extension, there is a homomorphism $\varphi : K \to L$, and φ is necessarily injective. For $a \in K$, $v \in L$, we define the scalar multiplication $a \cdot v$ to be

$$a \cdot v = \varphi(a)v.$$

With this definition of scalar multiplication, one verifies as an exercise that L is a vector space over K. □

Unless it will cause confusion, when $L : K$ is a field extension, we identify K with its isomorphic image in L; so for $a \in K, v \in L$, we write av for $a \cdot v$.

Definition. Suppose $L : K$ is a field extension. We define the degree of $L : K$ to be the dimension of L as a vector space over K. We use $[L : K]$ to denote the degree of $L : K$. We say $L : K$ is a finite extension if $[L : K] < \infty$.

Definition. We say $M : L : K$ is a tower of field extensions if $M : L$ and $L : K$ are field extensions, and in this case we say that L is an intermediate field (relative to the extension $M : K$).

Theorem 1.3. *(The Tower Law) Suppose $M : L : K$ is a tower of field extensions. Then $M : K$ is a field extension, and*

$$[M : K] = [M : L][L : K].$$

Proof. [Proved in Algebra 2] It is easy to check that $M : K$ is a field extension.

To show $[M : K] = [M : L][L : K]$, first suppose $[L : K] = r < \infty$ and $[M : L] = s < \infty$. Let $\{x_1, \ldots, x_r\}$ be a basis for L over K, $\{y_1, \ldots, y_s\}$ a basis for M over L. We verifies that

$$\mathcal{B} = \{x_i \cdot y_j : \ 1 \leq i \leq r, \ 1 \leq j \leq s \ \}$$

is a basis for M over K.

Suppose now that $[M : K] = n < \infty$. Thus there is a basis $\{z_1, \ldots, z_n\}$ for M over K. Since L contains (an isomorphic copy of) K, $\{z_1, \ldots, z_n\}$ spans M over L, and so $[M : L] \leq n < \infty$. Since L is a subspace of M, the dimension of L over K is bounded above by the dimension of M over K; so $[L : K] \leq n < \infty$. Thus by our preceding argument, since $[M : L], [L : K] < \infty$, we have $[M : K] = [M : L][L : K]$.

We can conclude from the above arguments that $[M : K] < \infty$ if and only if $[M : L], [L : K] < \infty$. Hence $[M : K] = \infty$ if and only if $[M : L] = \infty$ or $[L : K] = \infty$, and so we always have $[M : K] = [M : L][L : K]$. □

Remark. Suppose $L : K$ and $M : L$ are field extensions with $K \subseteq L \subseteq M$ and $[L : K] = [M : K] < \infty$. Then as vector spaces over K, L is a subspace of M of the same dimension as M, so L must equal M. If $L : K$ and $M : L$ are field extensions with the homomorphisms $\varphi : K \to L$ and $\psi : L \to M$, then we have $\psi \circ \varphi(K) \subseteq \psi(L) \subseteq M$, and as vector spaces over $\psi \circ \varphi(K)$, $\psi(L)$ is a subspace of M. So if $[L : K] = [M : K]$ then the dimension of $\psi(L)$ is the dimension of M, so $\psi(L) = M$.

Proved as an exercise in Algebra 2, one has the following.

Proposition 1.4. *Suppose K, L are fields and $\varphi : K \to L$ is a homomorphism. We extend φ to $\varphi : K[t] \to L[y]$ (where t, y are indeterminates) by defining*

$$\varphi(a_0 + a_1 t + \cdots + a_n t^n) = \varphi(a_0) + \varphi(a_1) y + \cdots + \varphi(a_n) y^n.$$

(Note that we are abusing notation here, using φ to denote two different functions.) Then $\varphi : K[t] \to L[y]$ is an injective homomorphism. Also, if $\varphi : K \to L$ is surjective, then $\varphi : K[t] \to L[y]$ is surjective and maps irreducible polynomials from $K[t]$ to irreducible polynomials in $L[y]$.

Definition. Say $L : K$ is a field extension (relative to the embedding φ) and $\alpha \in L$. We say α is algebraic over K if α is the root of $\varphi(f)$ for some (nonzero) $f \in K[t]$. When α is not algebraic over K, we say α is transcendental over K. When every element of L is algebraic over K, we simply say L is algebraic over K.

As discussed in Algebra 2, we have the following.

Proposition 1.5. *Suppose $L : K$ is a field extension with $K \subseteq L$, and $\alpha \in L$. We define $E_\alpha : K[t] \to L$ by $E_\alpha(f) = f(\alpha)$. Then E_α is a homomorphism.*

Proposition 1.6. *Let $L : K$ be a field extension with $K \subseteq L$ and $\alpha \in L$ so that α is algebraic over K. Then*

$$I = \{ f \in K[t] : \ f(\alpha) = 0 \ \}$$

is a nonzero ideal of $K[t]$, and there is a unique monic polynomial $m_\alpha(K) \in K[t]$ that generates I.

Proof. [Proved in Algebra 2] We have $I \neq \{0\}$ since α is algebraic over K. One easily checks that I is an ideal, and as $K[t]$ is a PID, I has a generator that can be scaled to be monic. If $(g) = I = (h)$ with g, h both monic, then we have $h = gx$, $g = hy$ for some $x, y \in K[t]$, and consequently $xy = 1$. Since h is monic, this means $x = 1$ and hence $g = h$. □

Definition. For $L : K$ a field extension with $\alpha \in L$ so that α is algebraic over K, the polynomial $m_\alpha(K)$ from the above proposition is called the minimal polynomial of α over K.

Theorem 1.7. *Suppose $L : K$ is a field extension, and $\alpha \in L$ is algebraic over K. Let $g = m_\alpha(K)$ (where $m_\alpha(K)$ is the minimal polynomial of α over K). Then g is irreducible over K, and $K[t]/(g)$ is a field.*

Proof. [Proved in Algebra 2] Identify K with its isomorphic image in L. Define $E_\alpha : K[t] \to L$ by $E_\alpha(f) = f(\alpha)$.

We have seen that E_α is a homomorphism, and

$$\ker E_\alpha = \{ f \in K[t] : \ f(\alpha) = 0 \ \} = (g)$$

where $g = m_\alpha(K)$. Thus by the Fundamental Homormorphism Theorem, $K[t]/(g)$ is isomorphic to a subring of L. Since L is an integral domain, $K[t]/(g)$ is an integral domain, and hence (g) is a prime ideal. We know $K[t]$ is a Euclidean domain and hence a PID, and in a PID any prime ideal is maximal. Thus (g) is a maximal ideal, so g is irreducible. Also, since (g) is maximal, $K[t]/(g)$ is a field. □

Theorem 1.8. *Let K be a field, $f \in K[t]$ irreducible. Then there exists a field extension $L : K$ relative to an embedding $\varphi : K \to L$ so that L contains a root of $\varphi(f)$.*

Proof. [Proved in Algebra 2] Set $L = K[t]/(f)$. Since f is irreducible and $K[t]$ is a Euclidean domain (and hence a PID), (f) is maximal. Thus L is a field.

Set $I = (f)$. With $\varphi : K \to L$ defined by $\varphi(c) = c + I$, it is easily verified that φ is a homomorphism, and hence $L : K$ is a field extension. We extend φ to a homomorphism from $K[t]$ to $L[y]$ by defining

$$\varphi\left(\sum_{j=0}^{n} c_j t^j\right) = \sum_{j=0}^{n} \overline{c}_j y^j$$

where $\overline{c} = \varphi(c)$. By Proposition 1.4, φ is an injective homomorphism.

Write

$$f = a_0 + a_1 t + \cdots + a_n t^n$$

where $a_0, a_1, \ldots, a_n \in K$ with $a_n \neq 0$. Let $\alpha = t + I$. Then with $(\varphi(f))(\alpha)$ denoting the polynomial $\varphi(f)$ evaluated at α, we have that

$$\begin{aligned}(\varphi(f))(\alpha) &= \sum_{j=0}^{n} \overline{a}_j \alpha^j \\ &= \sum_{j=0}^{n} (a_j + I)(t + I)^j \\ &= \sum_{j=0}^{n} (a_j t^j + I) \\ &= \left(\sum_{j=0}^{n} a_j t^j \right) + I \\ &= f + I \\ &= 0 + I\end{aligned}$$

since $f = \sum_{j=0}^{n} a_j t^j \in I$. Hence in L, α is a root of $\varphi(f)$. □

Definition. Let $L : K$ be a field extension, $\alpha \in L$. Assume $K \subseteq L$. Let $K[\alpha]$ denote the smallest subring of L containing K and α, and let $K(\alpha)$ be the smallest subfield of L containing K and α. More generally, suppose $A \subseteq L$. We let $K[A]$ denote the smallest subring of L containing K and A, and we let $K(A)$ denote the smallest subfield of L containing K and A.

As an exercise, one proves the following.

Proposition 1.9. *Let $L : K$ be a field extension so that $K \subseteq L$. Let $A \subseteq L$, and let*

$$\mathcal{C} = \{C \subseteq A : \ C \text{ is finite set } \}.$$

Then $K(A) = \cup_{C \in \mathcal{C}} K(C)$. Further, if $[K(C) : K] < \infty$ for all $C \in \mathcal{C}$, then $K(A) : K$ is an algebraic extension.

Proposition 1.10. *Let $L : K$ be a field extension, $\alpha \in L$. Assume $K \subseteq L$. Then*

$$K[\alpha] = \{c_0 + c_1\alpha + \cdots + c_d\alpha^d : \ d \in \mathbb{Z}_{\geq 0}, \ c_0, \ldots, c_d \in K \ \}$$

(which is $E_\alpha(K[t])$), and

$$K(\alpha) = \left\{ \frac{f}{g} : \ f, g \in K[\alpha], \ g \neq 0 \ \right\}.$$

Proof. [Proved in Algebra 2] Let

$$R = \{c_0 + c_1\alpha + \cdots + c_d\alpha^d : \ d \in \mathbb{Z}_{\geq 0}, \ c_0, \ldots, c_d \in K \ \}.$$

It is easy to check that R is a subring of L containing K and α. Also, given any subring R' of L containing K and α, and given any element f of R, we must have $f \in R'$ since R' contains K and α, and R' is closed under addition and multiplication. Thus any subring of L containing K and α necessarily contains R. Thus R is the smallest subring of L containing K and α.

Let Q be the field of fractions of $K[\alpha]$; so

$$Q = \left\{ \frac{f}{g} : \ f, g \in K[\alpha], \ g \neq 0 \right\}.$$

So Q is a subfield of L containing K and α. Suppose Q' is a subfield of L containing K and α. Certainly Q' contains $K[\alpha]$, and so for any $f, g \in K[\alpha]$ with $g \neq 0$, $f/g \in Q'$. So Q' must contain Q, and hence Q is the smallest subfield of L containing K and α.

□

Theorem 1.11. *Let $L : K$ be a field extension, $\alpha \in L$ algebraic over K. Assume $K \subseteq L$. Then $K[\alpha]$ is a field, and $K[\alpha] = K(\alpha)$. Further, with $n = \deg m_\alpha(K)$, we have that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over K, and hence $[K(\alpha) : K] = n$.*

Proof. [Proved in Algebra 2] We have seen that the evaluation map $E_\alpha : K[t] \to K[\alpha]$ is a homomorphism, and clearly it is surjective. We also know that $\ker E_\alpha = (m_\alpha(K))$ is a maximal ideal. So with $g = m_\alpha(K)$, we have $\psi : K[t]/(g) \to K[\alpha]$ is an isomorphism, given by $\psi(f + (g)) = E_\alpha(f)$, and $K[t]/(m_\alpha(K))$ is a field. Hence $K[\alpha]$ is a field, and $K[\alpha] = K(\alpha)$.

Given any $f \in K[t]$, there are $q, r \in K[t]$ so that $f = gq + r$ with $r = 0$ or $0 \leq \deg r < \deg g$. Then $f + (g) = r + (g)$. So given any $\beta \in K(\alpha)$, we have $E_\alpha(r + (g))$ for some $r \in K[t]$ with $r = 0$ or $0 \leq \deg r < n$; hence $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ spans $K(\alpha)$. We also know that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a linearly independent set, else α would be a root of some (nonzero) $h \in K[t]$ with $\deg h < \deg m_\alpha(K)$. □

Remark. This means that when $L : K$ is a field extension with $\alpha \in L$ algebraic over K and $n = \deg m_\alpha(K)$,

$$K(\alpha) = K[\alpha] = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} : \ c_0, \ldots, c_{n-1} \in K \ \}.$$

As exercises in Algebra 2, one proved the following two results.

Proposition 1.12. *Let $L : K$ be a field extension, $\alpha \in L$, and $K \subseteq L$. Then α is algebraic over K if and only if $[K(\alpha) : K] < \infty$.*

Proposition 1.13. *Let $L : K$ be a field extension, $\alpha \in L$ algebraic over K. Assume $K \subseteq L$. Then every element of $K(\alpha)$ is algebraic over K.*

As an exercise, one proves the following.

Theorem 1.14. *Let $L : K$ be a field extension, and assume $K \subseteq L$. The following are equivalent:*

(i) $[L : K] < \infty$.
(ii) *$L : K$ is an algebraic extension, and there are $\alpha_1, \ldots, \alpha_n \in L$ so that $L = K(\alpha_1, \ldots, \alpha_n)$ (where $K(\alpha_1, \ldots, \alpha_n)$ denotes the smallest subfield of L containing K and $\alpha_1, \ldots, \alpha_n$).*

As an exercise, one also proves the following.

Proposition 1.15. *Let $L : K$ be a field extension. Let*

$$L^{alg} = \{\alpha \in L : \ \alpha \text{ is algebraic over } K \ \}.$$

Then L^{alg} is a subfield of L.

We now recall some basic facts about finite fields.

Definition. Let K be a field with additive identity 0_K and multiplicative identity 1_K. We write $2\cdot 1_K$ to denote 1_K+1_K, $3\cdot 1_K$ to denote $1_K+1_K+1_K$, etc. We define the characteristic of K, denoted char$K$, to be the smallest positive integer n so that $n \cdot 1_K = 0_K$; if no such n exists, we define the characteristic of K to be 0.

Proposition 1.16. *Suppose K is a field.*

(a) *Suppose char$K > 0$; then char$K$ is prime.*
(b) *Suppose char$K = p > 0$; then for all $x \in K$, we have $p\cdot x = 0$ (where $p \cdot x = x + \cdots + x$, p times).*

Proof. [Proved in Algebra 2]

(a) Let $n = \text{char}K$. First note that since $1_K \neq 0_K$, we cannot have $n = 1$.

Suppose $n = km$ for some $k, m \in \mathbb{Z}_+$. One easily checks that $n \cdot 1_K = (k \cdot 1_K)(m \cdot 1_K)$. Since $n \cdot 1_K = 0_K$, we have $(k \cdot 1_K)(m \cdot 1_K) = 0_K$. Since $k\cdot 1_K, m\cdot 1_K \in K$ and K is an integral domain, we must have $k\cdot 1_K = 0_K$ or $m \cdot 1_K = 0_K$. By the definition of char$K$, n is the smallest positive integer so that $n \cdot 1_K = 0_K$; thus k or m must equal n, and hence n must be a prime.

(b) For any $x \in K$, we have

$$\begin{aligned} p \cdot x &= x + \cdots + x \ (p \text{ times}) \\ &= 1_K x + \cdots + 1_K x \ (p \text{ times}) \\ &= (p \cdot 1_K)x \\ &= 0_K x \\ &= 0_K, \end{aligned}$$

proving the claim. □

Theorem 1.17. *Suppose char$K = p > 0$. Set $F = \{c \cdot 1_K : \ c \in \mathbb{Z}\}$. Then F is a subfield of K, and is called the prime subfield of K. Further, $F \simeq \mathbb{Z}/p\mathbb{Z}$.*

Proof. Define $\eta : \mathbb{Z} \to K$ by $\eta(c) = c \cdot 1_K$. So $F = \eta(Z)$. One easily verifies that η is a ring homomorphism. Also, we know $p\mathbb{Z} \in \ker \eta$. So $\ker \eta$ is either $p\mathbb{Z}$ or $\mathbb{Z}$ (as these are the only ideals of $\mathbb{Z}$ containing $p\mathbb{Z}$). Since $\eta(1) = 1_K \neq 0_K$, we must have that $\ker \eta = p\mathbb{Z}$. Thus by the Fundamental Homomorphism Theorem, $F \simeq \mathbb{Z}/p\mathbb{Z}$. □

The proof of the next theorem relies on results from group theory.

Theorem 1.18. *Let K be a field; set $K^\times = K \setminus \{0\}$ (so $K^\times$ is an abelian group under multiplication). Suppose G is a finite subgroup of $K^\times$. Then G is cyclic. In particular, if K is a finite field then $K^\times$ is cyclic.*

Proof. [Proved in Algebra 2] Let $n = |G|$. Then there is some $x \in G$ so that for all $y \in G$, we have $\text{ord}(y) | \text{ord}(x)$. Let $k = \text{ord}(x)$; so by Lagrange's Theorem, $k|n$ and hence $k \leq n$. Also, for all $y \in G$, we have $\text{ord}(y)|k$ and thus $y \in G$ is a root of the polynomial $t^k - 1$. We have $G \subset K$ and $K[t]$ is a UFD; thus $t^k - 1$ can have at most k roots in K. Since every element

of G is a root of $t^k - 1$ and G has n elements, we must have $n \leq k$. Since we already established that $k \leq n$, we have $k = n$. So x is an element of G with order n, which means $\langle x \rangle$ is a cyclic subgroup of G with order n; since $n = |G|$, and so we must have $\langle x \rangle = G$. □

Finally, we recall some methods for testing polynomials for irreducibility.

Definitions. Let R be a UFD. We can extend the definition of hcf to an arbitrary (finite) number of elements $a_0, \ldots, a_n \in R$ provided they are not all 0: We set $c = \text{hcf}(a_0, \ldots, a_n)$ where $c \in R$ so that $c|a_i$ (for $0 \leq i \leq n$), and whenever $d|a_i$ (for $0 \leq i \leq n$), we have $d|c$. Suppose $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ with $f \neq 0$. We define the content of f to be $\text{hcf}(a_0, \ldots, a_n)$. We say $f \in R[X]$ is primitive if $f \neq 0$ and the content of f is 1.

Theorem 1.19. *(Gauss' Lemma) Suppose R is a UFD, Q its field of fractions. Suppose f is a primitive element of $R[X]$ with $\deg f > 0$. Then f is irreducible in $R[X]$ if and only if f is irreducible in $Q[X]$.*

Theorem 1.20. *(Eisenstein's Criterion) Suppose R is a UFD, $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ is primitive, and p is an irreducible element of R so that $p|a_i$ for $0 \leq i < n$, $p^2 \nmid a_0$, and $p \nmid a_n$. Then f is irreducible in $R[X]$ (and hence f is irreducible in $Q[X]$ where Q is the field of fractions of R).*

Theorem 1.21. *Let R be an integral domain, and I a prime ideal of R. Define $\varphi : R[X] \to (R/I)[X]$ by*

$$\varphi(a_0 + a_1X + \cdots + a_nX^n) = \overline{a}_0 + \overline{a}_1X + \cdots + \overline{a}_nX^n$$

where $\overline{a}_j = a_j + I$. Then φ is a surjective homomorphism. Suppose $f \in R[X]$ is primitive with its leading coefficient not in I; if $\varphi(f)$ is irreducible in $(R/I)[X]$, then f is irreducible in $R[X]$.

2. Ruler and compass constructions: an enhanced review

The topic of constructions by ruler (straight-edge) and compass is quite classical, and familiar to most of us from our early days in mathematics classes. Here we review basic constructions, and relate "constructible" points to the degree of a corresponding field extension of $\mathbb{Q}$.

From previous courses, we know that we can perform the following constructions:

(1) Bisect a given line segment.
(2) Bisect a given angle.
(3) Construct a line perpendicular to a given line or line segment.
(4) Construct a line parallel to a given line or line segment.
(1)](5)] Using a given line segment to define 1 unit of length, we can measure 1 unit in length on another given line or line segment.

Definition. A real number a is constructible if it is possible, using ruler and compass only, to construct a line segment of length $|a|$ in the plane where O is the origin, and where 1 unit in length is the distance from O to X.

Example. $\mathbb{Z}$ consists of constructible numbers. As proved in Algebra 2, we have the following result.

Proposition 2.1. *Let $a, b \in \mathbb{R}$ be nonzero constructible numbers, $a > 0$. Then*

$$a + b, ab, a/b, \sqrt{a}$$

are also constructible.

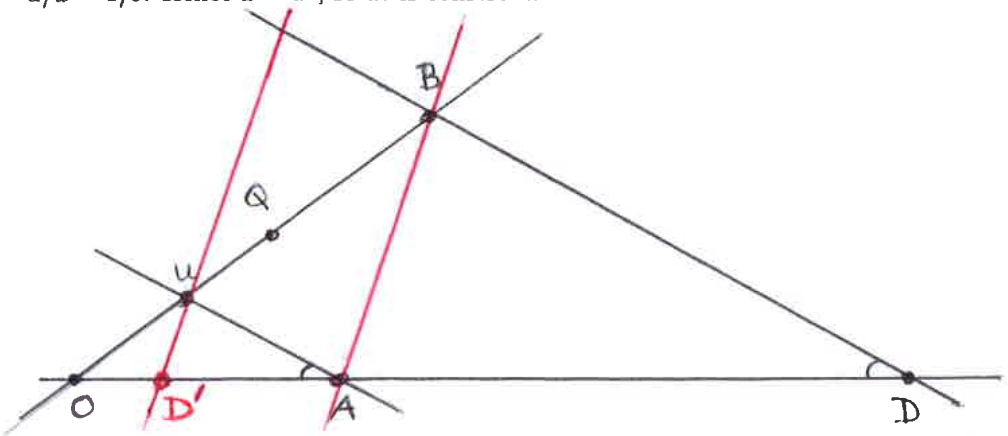
Proof. One shows as an exercise that $a + b$ is constructible.

To show $ab, a/b$ are constructible, it suffices to consider the case where $b > 0$. Then, to construct ab and a/b, we begin with a line segment OA of length a; fix a point Q not on the line through O and A. On the line through O and Q, fix points U and B so that the length of the segment OU is 1, and the length of the segment OB is b. Now construct the line L through B that is parallel to the line through A and U; let D be the point where L intersects the line through O and A. Let x denote the distance from O to D. Since the triangles $\triangle OAU$ and $\triangle ODB$ are similar, we have that $a/x = 1/b$; hence $x = ab$, so ab is constructible. [See the picture on the following page.] Now let L' be the line through U that is parallel to the line through A and B; let D' be the point where L' intersects the line through O and A, and let x' denote the distance from O to D'. Thus $\triangle OAB$ and $\triangle OD'U$ are similar triangles, so $x'/a = 1/b$; hence $x' = a/b$ and thus a/b is constructible. [See the picture on the following page.]

To construct $\sqrt{a}$, let A be a point on the ray beginning at O and passing through X so that the distance from X to A is a. Since we can bisect line segments, we can construct a circle of diameter $a + 1$ whose center is the midpoint of the line segment between O and A. Let L be the line passing through X that is perpendicular to the line through O and X. Let B be a point where L intersects the circle, and let x denote the distance from X to B. Since triangle $\triangle OBA$ is inscribed in a circle, with one side on a diameter of the circle, we know angle $\angle OBA$ is a right angle. Since they share angle $\angle BOX$ (which is the same as $\angle BOA$), triangles $\triangle OBA$ and $\triangle OXB$ are similar. Hence $\angle OAB$ is equal to $\angle OBX$. Also, $\angle OAB$ is the same as $\angle XAB$, so the triangles $\triangle XAB$ and $\triangle XBO$ are similar. Hence $1/x = x/a$, and from this we deduce $x^2 = a$, so $x = \sqrt{a}$. [See the picture on the following page.] $\square$

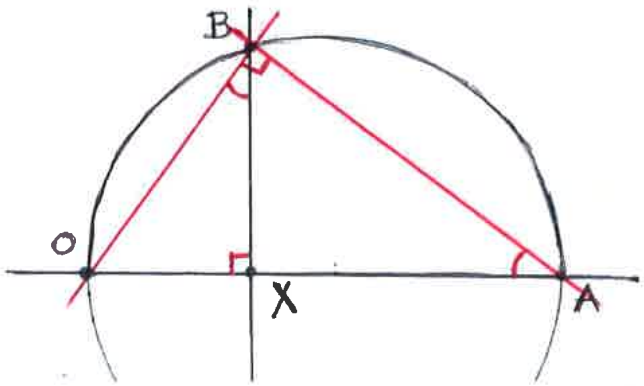
Suppose that $a, b \in \mathbb{R}_+$ are constructible. We show that ab, a/b, $\sqrt{a}$ are also constructible:

Let OA be a line segment of length a. Fix a point Q not on the line through O and A. On the line through O and Q, fix points U and B so that the length of the segment OU is 1, and the length of the segment OB is b. Now construct the line L through B that is parallel to the line through A and U; let D be the point where L intersects the line through O and A. Let x denote the distance from O to D (so x is constructible). Since the triangles $\triangle OAU$ and $\triangle ODB$ are similar, we have that $a/x = 1/b$. Hence $x = ab$, so ab is constructible.



Now let L' be the line through U that is parallel to the line through A and B; let D' be the point where L' intersects the line through O and A, and let x' denote the distance from O to D'. Thus $\triangle OAB$ and $\triangle OD'U$ are similar triangles, so $x'/a = 1/b$; hence $x' = a/b$ and thus a/b is constructible.

To construct $\sqrt{a}$, let A be a point on the ray beginning at O and passing through X so that the distance from X to A is a. Since we can bisect line segments, we can construct a circle of diameter $a+1$ whose center is the midpoint of the line segment between O and A. Let L be the line passing through X that is perpendicular to the line through O and X. Let B be a point where L intersects the circle, and let x denote the distance from X to B. Since triangle $\triangle OBA$ is inscribed in a circle, with one side on a diameter of the circle, we know angle $\angle OBA$ is a right angle. Since they share angle $\angle BOX$ (which is the same as $\angle BOA$), triangles $\triangle OBA$ and $\triangle OXB$ are similar. Hence $\angle OAB$ is equal to $\angle OBX$. Also, $\angle OAB$ is the same as $\angle XAB$, so the triangles $\triangle XAB$ and $\triangle XBO$ are similar. Hence $1/x = x/a$, and from this we deduce $x^2 = a$, so $x = \sqrt{a}$.



Definition. A point P is constructible if there exists a finite sequence $P_0, \ldots, P_n$ of points so that $P_0 = O$, $P_1 = X$, $P_n = P$, and the following property holds. For $1 \leq j \leq n$, let

$$S_j = \{P_0, \ldots, P_j\}.$$

For each j with $2 \leq j \leq n$, P_j is one of the following:

(i) the intersection of two distinct straight lines, each joining two points of S_{j-1};
(ii) a point of intersection of a straight line joining two points of S_{j-1} and a circle with centre a point of S_{j-1} and radius the distance between two points of S_{j-1};
(iii) a point of intersection of two distinct circles, each with centre a point of S_{j-1} and radius the distance between two points of S_{j-1}.

Also as proved in Algebra 2, we have the following theorem, and we recall its proof.

Theorem 2.2. *Let $P = (a, b)$ be a constructible point in the plane. Then*

$$[\mathbb{Q}(a, b) : \mathbb{Q}] = 2^t$$

for some non-negative integer t; here $\mathbb{Q}(a, b) = (\mathbb{Q}(a))(b)$.

Proof. Since P is constructible, there is a sequence of points $P_0, \ldots, P_n$ as in the above definition. Let $P_j = (a_j, b_j)$; set $K_1 = \mathbb{Q}$, and for $2 \leq j \leq n$, set

$$K_j = K_j(a_{j+1}, b_{j+1}) = \mathbb{Q}(a_1, b_1, \ldots, a_j, b_j).$$

We know

$$[K_n : \mathbb{Q}] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_2 : K_1].$$

We also know that $(a, b) = (a_n, b_n)$ and $[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(a, b)][\mathbb{Q}(a, b) : \mathbb{Q}]$. So $[\mathbb{Q}(a, b) : \mathbb{Q}]$ divides $[K_n : \mathbb{Q}]$, so if $[K_n : \mathbb{Q}]$ is a power of 2, so is $[\mathbb{Q}(a, b) : \mathbb{Q}]$. Thus to prove the theorem, it suffices to show that we have $[K_{j+1} : K_j] = 1$ or 2.

Case 1. Suppose (a_{j+1}, b_{j+1}) is the intersection of two straight lines, each joining points of S_j. So there are $(a_k, b_k), (a_m, b_m), (a_n, b_n), (a_r, b_r) \in S_j$ so that (a_{j+1}, b_{j+1}) is on the line through (a_k, b_k) and (a_m, b_m), and on the line through (a_n, b_n) and (a_r, b_r). Thus (a_{j+1}, b_{j+1}) is on the line described by

$$(Y - b_k)(a_m - a_k) = (X - a_k)(b_m - b_k),$$

or equivalently, (a_{j+1}, b_{j+1}) is a root of

$$(X - a_k)(b_m - b_k) - (Y - b_k)(a_m - a_k) \in K_j[X, Y].$$

Similarly, (a_{j+1}, b_{j+1}) is a root of

$$(X - a_n)(b_r - b_n) - (Y - b_n)(a_r - a_n) \in K_j[X, Y].$$

Solving, we find $a_{j+1}, b_{j+1} \in K_j$, so $[K_{j+1} : K_j] = 1$.

Case 2. Suppose (a_{j+1}, b_{j+1}) is a point of intersection of a line and a circle constructed using K_j. So there are $(a_k, b_k), (a_m, b_m), (a_n, b_n), (a_r, b_r), (a_s, b_s) \in S_j$ so that (a_{j+1}, b_{j+1}) is on the line through (a_k, b_k) and (a_m, b_m), and on

the circle with centre (a_n, b_n) and radius the distance between (a_r, b_r) and (a_s, b_s). Hence (a_{j+1}, b_{j+1}) is a root of

$$(X - a_k)(b_m - b_k) - (Y - b_k)(a_m - a_k) \in K_j[X, Y]$$

and of

$$(X - a_n)^2 + (Y - b_n)^2 - (a_r - a_s)^2 - (b_r - b_s)^2 \in K_j[X, Y].$$

Thus (a_{j+1}, b_{j+1}) is a root of polynomials of the form

$$uX + vY + w, X^2 + Y^2 + u'X + v'Y + w' \in K_j[X, Y].$$

First suppose $u \neq 0$. Then by solving $uX + vY + w = 0$ for X and substituting into the second polynomial, we obtain a quadratic polynomial $f \in K_j[Y]$. Suppose first that f has a root α in K_j; then $f = c(Y - \alpha)(Y - \beta)$ with $c, \alpha\beta \in K_j$. Thus $b_{j+1} = \alpha$ or β, so $b_{j+1} \in K_j$; solving for a_{j+1} we get $a_{j+1} \in K_j$. Now suppose f does not have a root in K_j; then since $\deg f = 2$, f is irreducible in K_j. We know b_{j+1} is a root of f, so $[K_j[b_{j+1}] : K] = \deg f = 2$. Now solving for a_{j+1}, we find $a_{j+1} \in K_j[b_{j+1}]$, so $K_{j+1} = K_j[a_{j+1}, b_{j+1}] = K_j[b_{j+1}]$. Hence $[K_{j+1} : K_j] = 2$.

Suppose $u = 0$; then we proceed as above with the roles of X and Y reversed.

Case 3. Suppose (a_{j+1}, b_{j+1}) is a point of intersection of two circles constructed using K_j; thus (a_{j+1}, b_{j+1}) is a root of two polynomials

$$X^2 + Y^2 + uX + vY + w, X^2 + Y^2 + u'X + v'Y + w' \in K_j[X, Y].$$

Hence (a_{j+1}, b_{j+1}) is a root of

$$(u - u')X + (v - v')Y + (w - w') \in K_j[X, Y].$$

We cannot have $u = u'$ and $v = v'$, else the circles would be concentric and thus would either be equal or have no point of intersection. So this case reduces to the previous case.

Thus in all cases, $[K_{j+1} : K_j] = 1$ or 2, so as discussed at the beginning of the proof, the theorem now follows. □

Using ruler and compass, we can construct an angle of $\pi/3$ radians: Take A to be the midpoint of the line segment joining O and X; so the distance from O to A is $1/2$. Construct a line L through A so that L is perpendicular to the line through O and X. Let B be a point on L of distance $\sqrt{3}/2$ from A. Then the angle $\angle AOB$ is $\pi/3$ radians. However, we have the following famous result.

Theorem 2.3. *An angle of $\pi/3$ radians cannot be trisected using ruler and compass constructions.*

Proof. Let A, B be the points described in the discussion above (so $\angle AOB$ is an angle of $\pi/3$ radians).

For the sake of contradiction, suppose we could trisect angle $\angle AOB$. Let $\alpha = \pi/9$, and let C be a point on the circle with centre O and radius 1 so that $\angle AOC = \alpha$. Let L' be the line through O and C; then the point $(\cos\alpha, \sin\alpha)$ is on the line L' and is distance 1 from O. Hence the point $(\cos\alpha, \sin\alpha)$ is

constructible. So $\cos\alpha, \sin\alpha$ lie in some field K where $[K:\mathbb{Q}] = 2^r$ for some non-negative r. This means we have

$$2^r = [K : \mathbb{Q}(\cos\alpha, \sin\alpha)][\mathbb{Q}(\cos\alpha, \sin\alpha) : \mathbb{Q}],$$

so $[\mathbb{Q}(\cos\alpha, \sin\alpha) : \mathbb{Q}] = 2^t$ for some non-negative $t \leq r$.

From the identity $\cos(3\theta) = 4(\cos\theta)^3 - 3\cos\theta$ and the fact that $\cos(\pi/3) = 1/2$, we have

$$4(\cos\alpha)^3 - 3\cos\alpha - \frac{1}{2} = 0.$$

With $\sigma = 2\cos\alpha$, we have $\sigma^3 - 3\sigma - 1 = 0$. As an exercise, one shows this polynomial is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(\sigma) : \mathbb{Q}] = 3$. By Theorem 2.2 we know $\alpha \in K$ where $K : \mathbb{Q}$ is a field extension with $[K : \mathbb{Q}] = 2^r$ for some non-negative integer r. We have $\sigma \in \mathbb{Q}(\alpha) \subseteq K$, so

$$2^r = [K : \mathbb{Q}] = [K : \mathbb{Q}(\sigma)][\mathbb{Q}(\sigma) : \mathbb{Q}].$$

This implies 3 divides 2^r, a contradiction.

This means we must not be able to trisect the angle $\pi/3$. □

As a final remark for this section, we note that if we can construct $\cos(2\pi/n)$ for $n \in \mathbb{Z}_+$, then we can construct a regular n-gon: Construct the circle of radius 1 and centre O. With $\alpha = 2\pi/n$, let A the the point of distance $\cos\alpha$ from O on the ray from O passing through X. Let L be the line through A perpendicular to the line through O and X, and let B_1 be a point where L intersects the circle. Then the arc on the circle between X and B has length α. Hence one can construct points $B_2, \ldots, B_{n-1}$ on the circle to partition the circle into arcs of length α. Constructing the line segments joining X to B_1, B_{n-1} to X, and B_j to B_{j+1} for $1 \leq j < n-1$ yields a regular n-gon inscribed in the circle.

(There are more results on possible/impossible contructions that are proved using results on "normal extensions" and "Galois extensions"; the interested reader can find an account of some such results in, for instance, the section *Geometric Constructions* in Grillet's book "Algebra".)

3. Extending field homomorphisms and the Galois group of an extension

Definitions. Let $L_1 : K_1$, $L_2 : K_2$ be field extensions relative to the embeddings $\varphi_i : K_i \to L_i$ $(i = 1, 2)$. Suppose $\sigma : K_1 \to K_2$ and $\tau : L_1 \to L_2$ are isomorphisms. We say τ extends σ if $\tau \circ \varphi_1 = \varphi_2 \circ \sigma$. (So when $K_1 \subseteq L_1$ and $K_2 \subseteq L_2$, this means that $\tau|_{K_1} = \sigma$, where $\tau|_{K_1}$ denotes τ restricted to K_1.) In the case that τ extends σ, we say $L_1 : K_1$ and $L_2 : K_2$ are isomorphic field extensions. With $L : K$ a field extension relative to the embedding $\varphi : K \to L$, $\sigma : M \to L$ a homomorphism where M is a subfield of L containing $\varphi(K)$, we say σ is a K-homomorphism if σ leaves $\varphi(K)$ pointwise fixed (meaning that for all $\alpha \in \varphi(K)$, $\sigma(\alpha) = \alpha$).

As an exercise, one proves the following.

Proposition 3.1. *Suppose $L : K$ is a field extension with $K \subseteq L$ and $\tau : L \to L$ is a K-homomorphism. Suppose $f \in K[t]$ with $\deg f \geq 1$ and $\alpha \in L$. If $f(\alpha) = 0$ then $f(\tau(\alpha)) = 0$. Thus for τ a K-automorphism of L, we have that $f(\alpha) = 0$ if and only if $f(\tau(\alpha)) = 0$.*

Theorem 3.2. *Suppose $\sigma : K_1 \to K_2$ is a field isomorphism, L_1, L_2 are fields with $K_i \subseteq L_i$ $(i = 1, 2)$, and $\alpha \in L_1$ is algebraic over K_1, $\beta \in L_2$ is algebraic over K_2. Then we can extend σ to an isomorphism $\tau : K_1(\alpha) \to K_2(\beta)$ so that $\tau(\alpha) = \beta$ if and only if $m_\beta(K_2) = \sigma(m_\alpha(K_1))$.*

Note: When $\tau : K_1(\alpha) \to K_2(\beta)$ is a homomorphism τ extending $\sigma : K_1 \to K_2$, τ is completely determined by σ and the value of $\tau(\alpha)$.

Proof. Suppose we have an isomorphism $\tau : K_1(\alpha) \to K_2(\beta)$ so that τ extends σ and $\tau(\alpha) = \beta$. Take $c_1, \ldots, c_d \in K$ so that $m_\alpha(K_1) = c_0 + c_1 t + \cdots + c_d t^d$ (so $c_d = 1$). Then

$$\begin{aligned} 0 &= \tau(c_0 + c_1\alpha + \cdots + c_d\alpha^d) \\ &= \tau(c_0) + \tau(c_1)\tau(\alpha) + \cdots + \tau(c_d)\tau(\alpha)^d \\ &= \sigma(c_0) + \sigma(c_1)\beta + \cdots + \sigma(c_d)\beta^d. \end{aligned}$$

Hence β is a root of $\sigma(m_\alpha(K_1))$. Since $m_\alpha(K_1)$ is monic and irreducible over K_1, $\sigma(m_\alpha(K_1))$ is monic and irreducible over K_2 (recall that $\sigma : K_1[t] \to K_2[t]$ is an isomorphism). Hence $\sigma(m_\alpha(K_1)) = m_\beta(K_2)$.

Now suppose β is a root of $\sigma(m_\alpha(K_1))$. To ease notation, let $f_1 = m_\alpha(K_1)$, $f_2 = \sigma(m_\alpha(K_1))$. So f_2 is monic and irreducible over K_2. We know the map $\psi_1 : K_1[t]/(f_1) \to K_1(\alpha)$ given by $\psi_1(g + (f_1)) = g(\alpha)$ is an isomorphism. Similarly, $\psi_2 : K_2[t]/(f_2) \to K_2(\beta)$ given by $\psi_2(h + (f_2)) = h(\beta)$ is an isomorphism. Define $\varphi : K_2[t] \to K_2[t]/(f_2)$ by $\varphi(h) = h + (f_2)$. One easily sees that φ is a surjective homomorphism. Thus $\varphi \circ \sigma : K_1[t] \to K_2[t]/(f_2)$ is a surjective homomorphism. We have

$$\begin{aligned} \ker \varphi \circ \sigma &= \{g \in K_1[t] : \ \sigma(g) + (f_2) = 0 + (f_2)\ \} \\ &= \{g \in K_1[t] : \ \sigma(g) \in (f_2)\ \} \\ &= \{g \in K_1[t] : \ \sigma(g) = f_2 h_2 \text{ for some } h_2 \in K_2[t]\ \} \\ &= \{g \in K_1[t] : \ g = \sigma^{-1}(f_2 h_2) \text{ for some } h_2 \in K_2[t]\ \} \\ &= \{g \in K_1[t] : \ g = f_1\sigma^{-1}(K_2[t])\ \} \\ &= (f_1) \end{aligned}$$

since $\sigma(K_1[t]) = K_2[t]$. Thus by the Fundamental Homomorphism Theorem, the map $\omega : K_1[t]/(f_1) \to K_2[t]/(f_2)$ defined by $\omega(g + (f_1)) = \sigma(g) + (f_2)$ is an isomorphism. So we have that $\tau : \psi_2 \circ \omega \circ \psi_1^{-1} : K_1(\alpha) \to K_2(\beta)$ is an isomorphism.

$$K_1(\alpha) \xrightarrow{\psi_1^{-1}} K_1[t]/(f_1) \xrightarrow{\omega} K_2[t]/(f_2) \xrightarrow{\psi_2} K_2(\beta)$$

Also, $\psi_2 \circ \omega \circ \psi_1^{-1}(\alpha) = \psi_2 \circ \omega(t + (f_1)) = \psi_2(\sigma(t) + (f_2)) = \psi_2(t + (f_2)) = \beta$, and for $c \in K_1$, $\psi_2 \circ \omega \circ \psi_1^{-1} = \psi_2 \circ \omega(c + (f_1)) = \psi_2(\sigma(c) + (f_2)) = \sigma(c)$. Thus τ extends σ, and $\tau(\alpha) = \beta$. □

Corollary 3.3. *Suppose that $L : M$ is a field extension with $M \subseteq L$, $\sigma : M \to L$ is a homomorphism, and $\alpha \in L$ is algebraic over M. Then the number of ways we can extend σ to a homomorphism $\tau : M(\alpha) \to L$ is the number of distinct roots of $\sigma(m_\alpha(M))$ that lie in L.*

Definitions. Suppose $L : K$ is a field extension. With $Aut(L)$ denoting the automorphism group of L, we set

$$Gal(L : K) = \{\sigma \in Aut(L) : \ \sigma \text{ is a } K\text{-homomorphism } \},$$

and we call $Gal(L : K)$ the Galois group of $L : K$. As an exercise, one shows that $Gal(L : K)$ is a subgroup of $Aut(L)$.

Note. Proposition 3.1 tells us that for $f \in K[t]$ and $\sigma \in Gal(L : K)$, σ permutes the roots of f that lie in L.

Theorem 3.4. *Suppose $L : K$ is an algebraic extension, and $\sigma : L \to L$ is a K-homomorphism. Then σ is an automorphism of L.*

Proof. Suppose first that $K \subseteq L$. Take $\alpha \in L$, and let

$$R = \{\beta \in L : \ \beta \text{ is a root of } m_\alpha(K) \ \}.$$

So over L,

$$m_\alpha(K) = g \cdot \prod_{\beta \in R} (t - \beta)^{r_\beta}$$

where the r_β are positive integers, and $g \in L[t]$ has no roots in L. We know

$$m_\alpha(K) = \sigma(m_\alpha(K)) = \sigma(g) \cdot \prod_{\beta \in R} (t - \sigma(\beta))^{r_\beta}.$$

Since $L[t]$ is a UFD, we must have that for some $\beta \in R$, $\sigma(\beta) = \alpha$ [and in fact $r_\beta = r_\alpha$]. This holds for all $\alpha \in L$, so $\sigma(L) = L$, and hence $\sigma \in Aut(L)$.

If $L : K$ is an extension relative to the embedding $\varphi : K \to L$ and φ is not the identity map, then we replace K by $\varphi(K)$ in the above argument. □

Theorem 3.5. *Suppose $L : K$ is a finite extension. Then $|Gal(L : K)| \leq [L : K]$.*

Proof. Suppose first that $K \subseteq L$. Thus $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in L$, where each α_i is algebraic over K (since $L : K$ is a finite extension). Let $K_0 = K_0' = K$, and for $1 \leq i \leq n$, let $K_i = K_{i-1}(\alpha_i)$. Let $\sigma_0 : K_0 \to K_0'$ be the identity map. We construct elements of $Gal(L : K)$ inductively as follows.

Suppose $\sigma_{i-1} : K_{i-1} \to K_{i-1}'$ is a isomorphism where K_{i-1}' is a subfield of L. Let $g_i = m_{\alpha_i}(K_{i-1})$, and let $g_i' = \sigma_{i-1}(g_i)$. (So g_i' is monic and irreducible.) Then we can extend σ_{i-1} to an isomorphism $\sigma_i : K_i \to K_i'$ for some subfield K_i' of L if and only if g_i' has a root in L; note that g_i' has at most $\deg g_i'$ roots in L, and $\deg g_i' = \deg g_i = [K_i : K_{i-1}]$. So there are at most $[K_i : K_{i-1}]$ ways to extend σ_{i-1} to σ_i.

Suppose we can extend σ_{i-1} to σ_i for $1 \leq i \leq n$; then we have a K-homomorphism $\sigma_n : K_n \to L$. Since $K_n = L$, σ_n is a K-homomorphism from L into L, and since $L : K$ is an algebraic extension, the previous theorem tells us that $\sigma \in Aut(L)$. Thus $\sigma_n \in Gal(L : K)$.

Note that this construction allows us to construct at most $[K_1 : K_0][K_2 : K_1] \cdots [K_n : K_{n-1}] = [L : K]$ elements of $Gal(L : K)$.

Now suppose $\tau \in Gal(L : K)$. Let $K_0 = K_0' = K$, and for $1 \leq i \leq n$, set $\beta_i = \tau(\alpha_i)$, $K_i = K_{i-1}(\alpha_i)$, $K_i' = K_{i-1}'(\beta_i)$, and let σ_i denote τ restricted to K_i. Thus for each i, σ_i extends σ_{i-1}, $\sigma_i(K_i) = K_i'$, and β_i is necessarily a root of $\sigma_i(g_i) = \tau(g_i)$ where $g_i = m_{\alpha_i}(K_{i-1})$. Hence each element of $Gal(L : K)$ can be constructed as previously described (i.e. by successively extending σ_{i-1} to σ_i for $1 \leq i \leq n$ where σ_0 is the identity map on K), and hence $|Gal(L : K)| \leq [L : K]$.

If $L : K$ is an extension relative to the embedding $\varphi : K \to L$ and φ is not the identity map, then we replace K by $\varphi(K)$ in the above argument. □

The proof of this theorem also gives us the following two corollaries.

Corollary 3.6. *Suppose $L : F$, $L : F'$ are finite extensions with $F \subseteq L$, $F' \subseteq L$, and $\psi : F \to F'$ an isomorphism. Then there are at most $[L : F]$ ways to extend ψ to a homomorphism from L into L.*

Corollary 3.7. *Suppose $L : K$ is a finite extension with $K \subseteq L$, and $\alpha_1, \ldots, \alpha_n \in L$ so that $L = K(\alpha_1, \ldots, \alpha_n)$. Let $K_0 = K$, and for $1 \leq i \leq n$, let $K_i = K_{i-1}(\alpha_i)$. Then every $\tau \in Gal(L : K)$ corresponds to a sequence of homomorphisms $\sigma_1, \ldots, \sigma_n$ so that $\sigma_0 : K \to L$ is the inclusion map, $\sigma_n = \tau$, and for $1 \leq i \leq n$, $\sigma_i : K_i \to L$ is a homomorphism extending $\sigma_{i-1} : K_{i-1} \to L$.*

4. Algebraic closures

Throughout, let K be a field.

In the introduction, we discussed how to construct an extension field L of a field K so that over L, a given nonconstant polynomial $f \in K[t]$ factors as a product of linear factors. More generally, we want to know the existence of an algebraic field extension $\overline{K} : K$ so that every nonconstant $f \in \overline{K}[t]$ factors in $\overline{K}[t]$ as a product of linear factors.

Definitions. We say a field M is algebraically closed if every nonconstant polynomial $f \in M[t]$ has a root in M. We say M is an algebraic closure of K if $M : K$ is an algebraic field extension so that M is algebraically closed.

As an exercise, one proves the following.

Lemma 4.1. *Let M be a field. The following are equivalent:*

(i) *M is algebraically closed.*
(ii) *Every nonconstant polynomial $f \in M[t]$ factors in $M[t]$ as a product of linear factors.*
(iii) *Every irreducible polynomial in $M[t]$ has degree 1.*
(iv) *The only algebraic extension of M is M itself.*

Lemma 4.2. *Let K be a field. There is an algebraic extension $E : K$ which contains a root of every irreducible $f \in K[t]$ (and hence for every $g \in K[t] \setminus K$).*

Proof. Let $\{q_i\}_{i\in\mathcal{I}}$ be the set of all irreducible polynomials over K ($\mathcal{I}$ some indexing set). Consider $R = K[\{t_i\}_{i\in\mathcal{I}}]$. Let A be the ideal of R generated by $\{q_i(t_i)\}_{i\in\mathcal{I}}$. We claim $A \neq R$: For the sake of contradiction, suppose $A = R$. So $1 \in A$, and hence

$$1 = \sum_{j\in\mathcal{J}} u_j q_j(t_j)$$

for some finite set $\mathcal{J}$, $\mathcal{J} \subseteq \mathcal{I}$, with $u_j \in R$. We can construct an extension $F : K$ so that for all $j \in \mathcal{J}$, q_j has a root $\alpha_j \in F$. Then we can define a homomorphism $\varphi : R \to F$ so that φ is the identity map on K, $\varphi(t_j) = \alpha_j$ for all $j \in \mathcal{J}$, and $\varphi(t_i) = 0$ for all $i \in \mathcal{I} \smallsetminus \mathcal{J}$. Then

$$1 = \varphi(1) = \sum_{j\in J} \varphi(u_j)\varphi(q_j)(\alpha_j) = \sum_{j\in\mathcal{J}} \varphi(u_j)q_j(\alpha_j) = 0,$$

a contradiction. So $A \neq R$.

Let B be a maximal ideal of R so that $A \subseteq B$ (such an ideal exists by Zorn's Lemma). Set $E = R/B$. So $E : K$ is a field extension relative to the embedding $\psi : K \to E$ defined by $\psi(c) = c + B$, and identify c with $\psi(c)$. Let $\alpha_i = t_i + B$ for all $i \in \mathcal{I}$. Define $\sigma : R \to E$ by $\sigma(u) = u + B$. So σ is a surjective homomorphism, and $\sigma(t_i) = \alpha_i$ for all $i \in \mathcal{I}$. Hence for all $i \in \mathcal{I}$,

$$\psi(q_i)(\alpha_i) = \sigma(q_i(t_i)) = q_i(t_i) + B = 0 + B$$

since $q_i(t_i) \in A \subseteq B$. Therefore every q_i has a root in E. Also, each α_i is algebraic over K, so $E = \psi(K)[\{\alpha_i\}_{i\in\mathcal{I}}]$ is an algebraic extension of K. □

Theorem 4.3. *For K a field, there is an algebraic extension $\overline{K}$ of K so that $\overline{K}$ is algebraically closed.*

Proof. We construct a sequence of fields $K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{n-1} \subseteq E_n \subseteq \cdots$ inductively: For $n \in \mathbb{Z}_+$, E_n is an algebraic extension of E_{n-1} containing a root of every $f \in E_{n-1}[t] \smallsetminus E_{n-1}$. So each E_n is algebraic over K. Hence $\overline{K} = \cup_{n\in\mathbb{Z}_+} E_n$ is algebraic over K. Suppose $f \in \overline{K}[t] \smallsetminus \overline{K}$. Since f has finitely many nonzero coefficients, $f \in E_{n-1}[t]$ for some $n \in \mathbb{Z}_+$. Therefore f has a root in $E_n \subseteq \overline{K}$. So $\overline{K}$ is algebraically closed. □

Corollary 4.4. *Let K be a field. Then $\overline{K}$ is a maximal algebraic extension of K.*

Theorem 4.5. *Let E be an algebraic extension of K with $K \subseteq E$, and let $\overline{K}$ be an algebraic closure of K. Given a homomorphism $\varphi : K \to \overline{K}$, φ can be extended to a homomorphism from E into $\overline{K}$.*

Proof. Let $\mathcal{S}$ be the set of all pairs (F, ψ) where F is a field with $K \subseteq F \subseteq E$, and $\psi : F \to \overline{K}$ is a homomorphism extending φ. Since $(K, \varphi) \in \mathcal{S}$, we have $\mathcal{S} \neq \emptyset$. We partially order $\mathcal{S}$ by defining $(F_1, \psi_1) \leq (F_2, \psi_2)$ if $F_1 \subseteq F_2$ and ψ_2 extends ψ_1. Suppose $\{(F_i, \psi)\}_{i\in I}$ is a (nonempty) chain in $\mathcal{S}$. Set $F = \cup_{i\in I} F_i$. So F is a subfield of E (check!). Define $\psi : F \to \overline{K}$ by $\psi(\alpha) = \psi_j(\alpha)$ where $j \in I$ so that $\alpha \in F_j$. Note that ψ is well-defined, for if $i, j \in I$ with $\alpha \in F_i$ and $\alpha \in F_j$, then either $(F_i, \psi_i) \leq (F_j, \psi_j)$ and hence ψ_j extends ψ_i, or vice versa. In either case, we have that $\psi_i(\alpha) = \psi_j(\alpha)$ for $\alpha \in F_i \cap F_j$. Also, ψ is a homomorphism extending ψ_i for all $i \in I$ (check!). Hence $(F, \psi) \in \mathcal{S}$. So every nonempty chain in $\mathcal{S}$ has an upper bound in

$\mathcal{S}$. Thus by Zorn's Lemma, $\mathcal{S}$ contains a maximal element (M, μ). Suppose $M \subsetneq E$. Take $\alpha \in E \setminus M$. Then α is algebraic over K and hence α is algebraic over M, so we can extend μ to a homomorphism $\nu : M(\alpha) \to \overline{K}$, giving us $(M(\alpha), \nu) \in \mathcal{S}$, and thereby contradicting that (M, μ) is a maximal element of $\mathcal{S}$. □

Corollary 4.6. *Suppose that $\overline{K}$ is an algebraic closure of K, and assume $K \subseteq \overline{K}$. Take $\alpha \in \overline{K}$ and suppose that $\sigma : K \to \overline{K}$ is a homomorphism. Then the number of (distinct) roots of $m_\alpha(K)$ in $\overline{K}$ is equal to the number of (distinct) roots of $\sigma(m_\alpha(K))$ in $\overline{K}$.*

Proof. In $\overline{K}[t]$, we have

$$m_\alpha(K) = \prod_{i=1}^{d} (t - \gamma_i)^{r_i}$$

where $\gamma_1, \ldots, \gamma_d$ are distinct, and $r_1, \ldots, r_d \in \mathbb{Z}_+$. By the previous theorem, we know we can extend σ to a homomorphism $\tau : \overline{K} \to \overline{K}$; recall that τ is necessarily injective. Then

$$\sigma(m_\alpha(K)) = \tau(m_\alpha(K)) = \prod_{i=1}^{d} (t - \tau(\gamma_i))^{r_i}.$$

Since τ is injective, $\tau(\gamma_1), \ldots, \tau(\gamma_d)$ are distinct, proving the corollary. □

As an exercise, one proves the following.

Proposition 4.7. *Suppose L, M are fields so that L is algebraically closed, and $\psi : L \to M$ is a homomorphism. Then $\psi(L)$ is algebraically closed.*

Proposition 4.8. *Suppose L, M are algebraic closures of K. Then $L \simeq M$.*

Proof. Identify K with its isomorphic image in L (so we assume $K \subseteq L$). We know that $M : K$ is an extension relative to some embedding $\varphi : K \to M$. Since L is an algebraic extension of K with $K \subseteq L$, we can extend φ to a homomorphism $\psi : L \to M$. Since L is a field, we know ψ must be injective. So $L \simeq \psi(L)$, and since L is algebraically closed, so is $\psi(L)$. Thus the only algebraic extension of $\psi(L)$ is $\psi(L)$. But $M : \psi(L)$ is an algebraic extension as $M : K$ is an algebraic extension, so we must have $M = \psi(L)$. □

As an exercise, one proves the following.

Proposition 4.9. *Suppose $L : K$ is an algebraic extension. Then $\overline{L}$ is an algebraic closure of K. Hence $\overline{L} \simeq \overline{K}$, and if $K \subseteq L \subseteq \overline{L}$, then we can take $\overline{K} = \overline{L}$.*

We now use the existence of algebraic closures to prove the following.

Proposition 4.10. *Suppose $L : K$ is an extension with $K \subseteq L$, $g \in L[t]$ is irreducible over L, and in $L[t]$, $g | f$ where $f \in K[t]$ ($f \neq 0$). Then g divides a factor of f that is irreducible over K. That is, there is some $h \in K[t]$ so that h is irreducible over K, $h | f$ in $K[t]$, and $g | h$ in $L[t]$.*

Proof. Assume $K \subseteq L \subseteq \overline{L}$ where $\overline{L}$ is some algebraic closure of L. As g is irreducible over L, we know $\deg g \geq 1$. Thus there is some $\alpha \in \overline{L}$ so that $g(\alpha) = 0$. Thus in $\overline{L}$, $f(\alpha) = 0$. So α is algebraic over K, and f is in the ideal of $K[t]$ generated by $h = m_\alpha(K)$. Hence h is irreducible over K and $h|f$. Somewhat similarly, since $h(\alpha) = 0$, h is in the ideal of $L[t]$ generated by $m_\alpha(L)$, and so $m_\alpha(L)|h$. Since g is irreducible over L with $g(\alpha) = 0$, we have $g = \lambda m_\alpha(L)$ where $\lambda \in L^\times$ is the leading coefficient of g. Therefore $g|h$, as desired. □

5. Splitting field extensions

Throughout, K is a field.

Definitions. Suppose $L : K$ is a field extension relative to the embedding $\varphi : K \to L$ and $f \in K[t] \smallsetminus K$. We say f splits over L if

$$\varphi(f) = \varphi(\lambda)(t - \alpha_1) \cdots (t - \alpha_n)$$

where $\lambda \in \varphi(K)$ and $\alpha_1, \ldots, \alpha_n \in L$. So when $K \subseteq L$, f splits over L if

$$f = \lambda(t - \alpha_1) \cdots (t - \alpha_n)$$

where $\lambda \in K$ and $\alpha_1, \ldots, \alpha_n \in L$. Suppose that f splits over L (note that f will split over an algebraic closure of K); with M a field so that $\varphi(K) \subseteq M \subseteq L$, we say $M : K$ is a splitting field extension for f if M is the smallest subfield of L containing $\varphi(K)$ over which f splits. (So with $M : K$ a splitting field extension for f and $\varphi(K) \subseteq M \subseteq L$, if F is a field with $\varphi(K) \subseteq F \subseteq L$ so that f splits over F, then $M \subseteq F$.) More generally, suppose $S \subseteq K[t] \smallsetminus K$ so that every $f \in S$ splits over L; with M a field so that $\varphi(K) \subseteq M \subseteq L$, we say $M : K$ is a splitting field extension for S if M is the smallest subfield of L containing $\varphi(K)$ over which every nonconstant polynomial $f \in S$ splits. (So with $M : K$ a splitting field extension for S and $\varphi(K) \subseteq M \subseteq L$, if F is a field with $\varphi(K) \subseteq F \subseteq L$ so that every polynomial in S splits over F, then $M \subseteq F$.)

The next proposition is simple and intuitive, but useful to record.

Proposition 5.1. *Suppose $L : K$ is a splitting field extension for $f \in K[t] \smallsetminus K$ (with $L : K$ an extension relative to the embedding $\varphi : K \to L$). Let $\alpha_1, \ldots, \alpha_n \in L$ be the roots of $\varphi(f)$. Then $L = \varphi(K)(\alpha_1, \ldots, \alpha_n)$.*

Proof. Identify K with its isomorphic image in L so that we can assume $K \subseteq L$. Set $F = K(\alpha_1, \ldots, \alpha_n)$. Thus $K \subseteq F \subseteq L$ and f splits over F. Since $L : K$ is a splitting field extension for f, we must have $L \subseteq F$. Hence $L = F = K(\alpha_1, \ldots, \alpha_n)$. □

Remark. Suppose $L : K$ is a splitting field extension for some $f \in K[t] \smallsetminus K$. Then by Proposition 3.1, and recalling that field homomorphisms are necessarily injective, each element of $Gal(L : K)$ permutes the roots of f, and hence corresponds to an element of the permutation group S_d where d is the number of (distinct) roots of f. Consequently $Gal(L : K)$ corresponds to a subgroup of S_d.

As an exercise, one proves the following.

Proposition 5.2. *Suppose $L : K$ is a splitting field extension for $f \in K[t] \setminus K$. Then $[L : K] \leq (\deg f)!$.*

Remark. One can actually prove that with $L : K$ a splitting field extension for some (nonconstant) $f \in K[t]$ with $\deg f = n$, one has that $[L : K]$ divides $n!$. (The proof of this uses the fact that $k!m!$ divides $(k + m)!$ since the binomial coefficient $\binom{m+k}{k}$ is an integer.)

In the introduction, we presented an algorithm to construct a splitting field extension $L : K$ for some $f \in K[t]$. Here we present a more general result; the proof takes advantage of the existence of algebraic closures.

Proposition 5.3. *Given $S \subseteq K[t] \setminus K$, there exists a splitting field extension $L : K$ for S, and $L : K$ is an algebraic extension. More explicitly, suppose $\overline{K}$ is an algebraic closure of K so that $\overline{K} : K$ is an extension relative to the embedding $\varphi : K \to \overline{K}$. Let*

$$A = \{\alpha \in \overline{K} : \ \alpha \text{ is a root of some } \varphi(f) \in \varphi(S) \ \}.$$

Then with $K' = \varphi(K)$, $K'(A) : K$ is a splitting field extension for S.

Proof. Let $\overline{K}$ be an algebraic closure of K; identify K with its isomorphic image in $\overline{K}$ to assume $K \subseteq \overline{K}$. Thus for every $f \in S$, f splits over $\overline{K}$. Let

$$A = \{\alpha \in \overline{K} : \ \alpha \text{ is a root of some } f \in S \ \}.$$

(So every element of A is algebraic over K.) Thus with $K(A)$ the smallest subfield of $\overline{K}$ containing K and A, every $f \in S$ splits over $K(A)$. Also, since $\overline{K}$ is a field and hence $\overline{K}[t]$ is a UFD, any subfield of $\overline{K}$ containing K over which every nonzero $f \in S$ splits must contain A; hence such a subfield of $\overline{K}$ must contain $K(A)$. Thus $K(A) : K$ is a splitting field extension for S. To see that $K(A) : K$ is algebraic, choose $\beta \in K(A)$. Thus by Proposition 1.9, $\beta \in K(C)$ where C is a finite subset of A. So C is a finite subset consisting of elements that are algebraic over K; hence $[K(C) : K] < \infty$, and so $K(C) : K$ is an algebraic extension. Thus, since $\beta \in K(C)$, β is algebraic over K.

If we do not assume $K \subseteq \overline{K}$, then we replace K by $K' = \varphi(K)$ in the above argument. □

Theorem 5.4. *Suppose that $f \in K[t] \setminus K$, and suppose that $L : K$, $M : K$ are splitting field extensions for f. Then $L \simeq M$ (hence $[L : K] = [M : K]$).*

Proof. Identify K with its isomorphic image in L. We have that $M : K$ is an extension relative to an embedding $\varphi : K \to M$, and f splits over M. Let $K' = \varphi(K)$, $f' = \varphi(f)$, and let $\alpha_1, \ldots, \alpha_n \in L$ be the roots of f in L (and thus $L = K(\alpha_1, \ldots, \alpha_n)$).

Proof 1 that $L \simeq M$: Let $K_0 = K$, and for $1 \leq i \leq n$, let $K_i = K_{i-1}(\alpha_i)$ and $g_i = m_{\alpha_i}(K_{i-1})$. So with $g_1' = \varphi(g_1) \in K'[t]$, g_1' is a monic factor of $f' = \varphi(f)$ that is irreducible over K'. Let $\beta_1 \in M$ be a root of g_1' (such β_1 exists since f' splits over M, and since $M[t]$ is a UFD, g_1' also splits over M). Let $\varphi_1 : K_1 \to K_1' = K'(\beta_1)$ be the isomorphism extending φ so that $\varphi_1(\alpha_1) = \beta_1$. We proceed inductively: For $1 < i \leq n$, suppose $\varphi_{i-1} : K_{i-1} \to K_{i-1}'$ is an isomorphism extending φ. Since $g_i | f$, we have

$g_i' | f'$. Since f' splits over M, there is some $\beta_i \in M$ so that β_i is a root of g_i' and thus (by Theorem 3.2) we can extend φ_{i-1} to an isomorphism $\varphi_i : K_i \to K_i' = K_{i-1}'(\beta_i)$ so that $\varphi_i(\alpha_i) = \beta_i$. Thus (recalling that $K_n = L$) $\varphi_n : L \to K_n' = K'(\beta_1, \ldots, \beta_n)$ is an isomorphism extending φ with $\varphi(\alpha_i) = \beta_i$ for $1 \leq i \leq n$. In $L[t]$ we have

$$f = \lambda \prod_{i=1}^{n} (t - \alpha_i)^{r_i}$$

for some $r_i \in \mathbb{Z}_+$ and $\lambda \in K$. So

$$f' = \varphi(f) = \varphi_n(f) = \varphi(\lambda) \prod_{i=1}^{n} (t - \beta_i)^{r_i}.$$

Hence $K_n' : K$ is a splitting field extension for f, where the extension is relative to the embedding φ, and $K_n' \subseteq M$. Since $M : K$ is a splitting field extension for f, where the extension is relative to the embedding φ, we must have $K_n' = M$. Thus $\varphi_n : L \to M$ is an isomorphism.

Proof 2 that $L \simeq M$: Let $\overline{M}$ be an algebraic closure of M, and assume that $M \subseteq \overline{M}$. Thus $\overline{M} : M$ and $M : K$ are algebraic extensions, so $\overline{M} : K$ is an algebraic extension. Since $\overline{M}$ is algebraically closed, this means that $\overline{M}$ is an algebraic closure of K. We have a homomorphism $\varphi : K \to M \subseteq \overline{M}$ and we know that $L : K$ is an algebraic extension. Thus by Theorem 4.5, we can extend φ to a homomorphism $\psi : L \to \overline{M}$. For $1 \leq i \leq n$, let $\beta_i = \psi(\alpha_i)$. In $L[t]$, we have

$$f = \lambda \prod_{i=1}^{n} (t - \alpha_i)$$

where $\lambda \in K$, so

$$f' = \varphi(f) = \psi(f) = \varphi(\lambda) \prod_{i=1}^{n} (t - \beta_i).$$

Hence f' splits over $K'(\beta_1, \ldots, \beta_n)$. Since $\overline{M}[t]$ is a UFD and f' splits over M, we must have $\beta_1, \ldots, \beta_n \in M$. Also, $K' = \varphi(K) \subseteq M$, so $K'(\beta_1, \ldots, \beta_n) \subseteq M$. Since $M : K$ is a splitting field extension for f, we must have $K'(\beta_1, \ldots, \beta_n) = M$. Finally, note that $\psi(L) = \psi(K(\alpha_1, \ldots, \alpha_n)) = K'(\beta_1, \ldots, \beta_n)$ (recall that ψ extends φ). Since ψ is an injective homomorphism, we have $L \simeq M$.

To see that $[L : K] = [M : K]$, one checks that φ_n maps a basis for L as a vector space over K to a basis for M as a vector space over K. □

More generally, one proves the following as an exercise.

Theorem 5.5. *Suppose that $S \subseteq K[t]$, and suppose that $L : K$, $M : K$ are splitting field extensions for S. Then $L \simeq M$ and $[L : K] = [M : K]$*

Example. Let $f = t^4 - 2 \in \mathbb{Q}[t]$. Let $\alpha = \sqrt[4]{2} \in \mathbb{R}_+$. Then $-\alpha, i\alpha, -i\alpha$ are also roots of f (here $i = \sqrt{-1}$). We see that f is irreducible over $\mathbb{Z}$ by Eisenstein's criterion (with $p = 2$), and thus irreducible over $\mathbb{Q}$ by Gauss' Lemma. So $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Also, $\mathbb{Q}(\alpha, i\alpha) : \mathbb{Q}$ is a splitting field

extension for f. Note that $i\alpha \cdot \alpha^3 = 2i \in \mathbb{Q}(\alpha, i\alpha)$, so $i \in \mathbb{Q}(\alpha, i\alpha)$ and hence $\mathbb{Q}(\alpha, i) \subseteq \mathbb{Q}(\alpha, i\alpha)$. Clearly $\mathbb{Q}(\alpha, i\alpha) \subseteq \mathbb{Q}(\alpha, i)$ so $\mathbb{Q}(\alpha, i\alpha) = \mathbb{Q}(\alpha, i)$. Hence

$$[\mathbb{Q}(\alpha, i\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

We know that i is a root of $t^2 + 1$, so $m_i(\mathbb{Q}(\alpha))$ divides $t^2 + 1$. Hence $\deg m_i(\mathbb{Q}(\alpha)) = 1$ or 2. If $\deg m_i(\mathbb{Q}(\alpha)) = 1$ then $i \in \mathbb{Q}(\alpha)$, but $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ and $i \notin \mathbb{R}$. So $m_i(\mathbb{Q}(\alpha))$ must equal $t^2 + 1$, and hence $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$. Consequently $[\mathbb{Q}(\alpha, i\alpha) : \mathbb{Q}] = 8$.

To construct the elements of $Gal(\mathbb{Q}(\alpha, i) : \mathbb{Q})$, we first construct each $\mathbb{Q}$-homomorphism $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha, i)$, then we extend σ to a homomorphism $\tau : \mathbb{Q}(\alpha, i) \to \mathbb{Q}(\alpha, i)$. Then by Theorem 3.4, $\tau \in Aut(\mathbb{Q}(\alpha, i))$, and hence $\tau \in Gal(\mathbb{Q}(\alpha, i) : \mathbb{Q})$. We also know from Corollary 3.7 that every element of $Gal(\mathbb{Q}(\alpha, i) : \mathbb{Q})$ can be constructed in this way. We know that $\sigma(\alpha)$ must be a root of $m_\alpha(\mathbb{Q})$.

For instance, we can define $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha, i)$ by determining that $\sigma(\alpha) = i\alpha$. We know that $\{1, \alpha, \alpha^2, \alpha^3\}$ is a basis for $\mathbb{Q}(\alpha) : \mathbb{Q})$, so σ is given by

$$\begin{aligned}\sigma(a + b\alpha + c\alpha^2 + d\alpha^3) &= a + bi\alpha + c(i\alpha)^2 + d(i\alpha)^3 \\ &= a + bi\alpha - c\alpha^2 - di\alpha^3.\end{aligned}$$

Then we can extend σ to $\tau : \mathbb{Q}(\alpha, i) \to \mathbb{Q}(\alpha, i)$ by determining that $\tau(i) = -i$. As $\{1, i\}$ is a basis for $\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)$, τ is given by

$$\tau(u + iv) = \sigma(u) - i\sigma(v)v$$

where $u, v \in \mathbb{Q}(\alpha)$. [We know by Theorem 3.4 that $\tau \in Aut(\mathbb{Q}(\alpha, i))$, but we can also see this by noting that

$$\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$$

is a basis for $\mathbb{Q}(\alpha, i) : \mathbb{Q}$, and

$$\begin{aligned}&\{\tau(1), \tau(\alpha), \tau(\alpha^2), \tau(\alpha^3), \tau(i), \tau(i\alpha), \tau(i\alpha^2), \tau(i\alpha^3)\} \\ &\quad = \{1, i\alpha, -\alpha^2, -i\alpha^3, -i, \alpha, -i\alpha^2, \alpha^3\}\end{aligned}$$

is also a basis for $\mathbb{Q}(\alpha, i) : \mathbb{Q}$, so τ must be bijective.] We know that each element of $Gal(\mathbb{Q}(\alpha, i) : \mathbb{Q})$ corresponds to a permutation of the roots of f; this function τ corresponds to the permutation $(\alpha \ \ i\alpha)(-\alpha \ \ -i\alpha)$.

As an exercise, one computes the subgroup of S_4 to which $Gal(\mathbb{Q}(\alpha, i) : \mathbb{Q})$ is isomorphic.

6. Normal extensions and compositums

Definition. An extension $L : K$ is a normal extension if $L : K$ is algebraic and every irreducible $f \in K[t]$ either splits over L or has no root in L.

As an exercise, one proves the following.

Proposition 6.1. *Suppose $L : K$ is a normal extension. Assume that $K \subseteq L \subseteq \overline{K}$. (Recall that since $L : K$ is algebraic, any algebraic closure of K is an algebraic closure of L.) Then for any K-homomorphism $\tau : L \to \overline{K}$, we have $\tau(L) = L$.*

Proposition 6.2. *An extension $L : K$ is a finite, normal extension if and only if it is a splitting field extension for some $f \in K[t] \setminus K$. More generally, an extension $L : K$ is normal if and only if it is a splitting field extension for some $S \subseteq K[t] \setminus K$.*

Proof. Assume $K \subseteq L \subseteq \overline{K}$ where $\overline{K}$ is a fixed algebraic closure of K. We first consider the case where $L : K$ is a finite extension.

Suppose that $L : K$ is a finite, normal extension (and thus $L : K$ is necessarily algebraic). Since $[L : K] < \infty$, there are $\alpha_1, \ldots, \alpha_n \in L$ so that $L = K(\alpha_1, \ldots, \alpha_n)$. Let

$$f = m_{\alpha_1}(K) \cdots m_{\alpha_n}(K).$$

So $f \in K[t] \setminus K$, and each irreducible factor $m_{\alpha_i}(K)$ of f has a root α_i in L. Since $L : K$ is normal, each $m_{\alpha_i}(K)$ must split over L ($1 \leq i \leq n$), and hence f must split over L. With $\alpha_1, \ldots, \alpha_n, \ldots, \alpha_r \in L$ all the roots of f, we have

$$K(\alpha_1, \ldots, \alpha_r) = L,$$

so by Proposition 5.1, $L : K$ is a splitting field extension for f.

Now suppose $L : K$ is a splitting field extension for some $f \in K[t] \setminus K$; note that Proposition 5.1 implies that $[L : K] < \infty$. Suppose $g \in K[t]$ is irreducible over K and has a root $\gamma \in L$. Let $\delta \in \overline{K}$ be a root of g. Thus, with $\lambda \in K$ the leading coefficient of g,

$$\lambda m_\alpha(K) = g = \lambda m_\beta(K).$$

Hence by Theorem 3.2, we can extend the identity map on K to an isomorphism $\sigma : K(\gamma) \to K(\delta)$ so that $\sigma(\gamma) = \delta$. Also, we have $L = K(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n \in \overline{K}$ are the distinct roots of f (and hence are algebraic over K and over $K(\gamma)$). As $L(\gamma) : K(\gamma)$ is algebraic, by Theorem 4.5 we can extend σ to a homomorphism $\tau : L(\gamma) \to \overline{K}$. As τ extends the identity map on K, for $1 \leq i \leq n$ we have

$$0 = \tau(f(\alpha_i)) = f(\tau(\alpha_i)).$$

Hence, as τ is injective, $\tau(\alpha_1), \ldots, \tau(\alpha_n) \in \overline{K}$ are distinct roots of f. Since $\overline{K}[t]$ is a UFD, we must have $\{\tau(\alpha_1), \ldots, \tau(\alpha_n)\} = \{\alpha_1, \ldots, \alpha_n\}$. Thus $\tau(L) = L$ and so by Theorem 3.4, $\tau \in Aut(L)$. Hence τ is an extension of the automorphism $\tau|_L$ of L with $\tau(\gamma) = \delta$, so by Theorem 3.2, $m_\delta(L) = \tau|_L(m_\gamma(L)) = \tau(m_\gamma(L))$. Thus $[L(\gamma) : L] = \deg m_\gamma(L) = [L(\delta) : L]$. But $\gamma \in L$, so $1 = [L(\gamma) : L] = [L(\delta) : L]$, which means that $\delta \in L$. This holds for all roots $\delta \in \overline{K}$ of g, so g splits over L. This holds for all irreducible $g \in K[t]$ that have a root in L, and hence $L : K$ is a normal extension.

Now suppose $L : K$ is normal (and thus algebraic). Let

$$S = \{g \in K[t] : \ g \text{ is irrediculble in } K[t] \text{ and } g(\alpha) = 0 \text{ for some } \alpha \in L \ \}.$$

Thus every element of S splits over L. As an exercise, one checks that $L : K$ is a splitting field extension for S.

Suppose $L : K$ is a splitting field extension for some $S \subseteq K[t] \setminus K$, and $g \in K[t]$ so that g is irreducible over K with $g(\gamma) = 0$ for some $\gamma \in L$. By

Proposition 5.3, $[L : K]$ is algebraic. Also, by Proposition 1.9, $\gamma \in K(D)$ where D is a finite subset of

$$A = \{\beta \in L : \ \beta \text{ is a root of some } f \in S \ \}.$$

(Note that $L = K(A)$.) For each $\beta \in D$, choose $f_\beta \in S$ so that β is a root of f_β. Let $D' \subseteq \overline{K}$ be the set of all roots of $\{f_\beta : \ \beta \in D \ \} \subseteq S$. So D' is a finite set, and $D \subseteq D' \subseteq L$ with $K(D') : K$ a splitting field extension for $h = \prod_{\beta \in D} f_\beta$. Hence $K(D') : K$ is a finite, normal extension with $\gamma \in D'$. Thus g splits over $K(D')$, and hence over L. Therefore $L : K$ is a normal extension. □

As an exercise, one proves the following.

Proposition 6.3. *Suppose $L : M : K$ is a tower of field extensions and $L : K$ is a normal extension. Then $L : M$ is also a normal extension.*

Theorem 6.4. *Suppose that $M : K$ is a normal extension, and that L is an intermediate field, meaning that $M : L$ and $L : K$ are field extensions. Then the following are equivalent:*

(i) *The field extension $L : K$ is normal.*
(ii) *Any K-homomorphism of L into M is an automorphism of L.*
(iii) *Whenever $\sigma : M \to M$ is a K-automorphism, we have $\sigma(L) \subseteq L$.*

Proof. We identify K, L with their isomorphic images in M and M with its isomorphic image in $\overline{K}$ to assume that $K \subseteq L \subseteq M \subseteq \overline{K}$. Note that since $M : K$ is an algebraic extension, so is $L : K$.

To show (i) imples (iii): Suppose that (i) holds, and that $\sigma : M \to M$ is a K-automorphism. Take $\alpha \in L$, and let $g = m_\alpha(K)$. Then

$$g(\sigma(\alpha)) = \sigma(g(\alpha)) = \sigma(0) = 0,$$

and so $\sigma(\alpha)$ is a root of g. Since $L : K$ is normal, this means that $\sigma(\alpha) \in L$. As this holds for all $\alpha \in L$, we have $\sigma(L) \subseteq L$.

To show (iii) implies (ii): Suppose that (iii) holds, and that $\psi : L \to M$ is a K-homomorphism. Since $M : K$ is an algebraic extension, so is $M : L$. Thus by Theorem 4.5, we can extend ψ to a homomorphism $\sigma : M \to \overline{K}$. Since σ is a K-homomorphism and $M : K$ is normal, by Proposition 6.1 we have that $\sigma(M) = M$. Having assumed (iii), we have $\psi(L) = \sigma(L) \subseteq L$. Then by Theorem 3.4, $\psi \in Aut(L)$.

To show (ii) implies (i): Suppose that (ii) holds, and that $g \in K[t]$ is irreducible over K so that g has a root α in L. Thus for λ the leading coefficient of g, we have $g = \lambda m_\alpha(K)$. Take $\beta \in M$ a root of g. Thus $m_\beta(K) = \lambda^{-1} g = m_\alpha(K)$. Hence by Theorem 3.2, there is a K-isomorphism $\psi : K(\alpha) \to K(\beta)$ so that $\psi(\alpha) = \beta$. By Theorem 4.5, we can extend ψ to a homomorphism $\sigma : L \to \overline{K}$, and we can extend σ to a homomorphism $\tau : M \to \overline{K}$. Then by Proposition 6.1, $\tau(M) = M$. Hence

$$\sigma(L) = \tau(L) \subseteq \tau(M) = M.$$

Having assumed (ii), we find that $\sigma \in Aut(L)$. Thus $\beta = \sigma(\alpha) \in L$. As g splits over M, this holds for all roots β of g, so g splits over L. As this holds for all $g \in K[t]$ that are irreducible over K, we have that $L : K$ is normal. □

Definition. Let $L : K$ be an algebraic extension, and assume $K \subseteq L$. A normal closure of $L : K$ is a field M so that $M : L$ is an extension, $M : K$ is a normal extension, and if $N \subseteq M$ so that $N : L$ is an extension and $N : K$ is a normal extension, then $N = M$.

Proposition 6.5. *Suppose $L : K$ is an algebraic extension. Then there exists a normal closure M of $L : K$. When $L : K$ is finite, so is $M : K$.*

Proof. Assume $K \subseteq L \subseteq \overline{K}$.

First suppose that $L : K$ is a finite extension. Thus $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in L$. Let $f = m_{\alpha_1}(K) \cdots m_{\alpha_n}(K)$, and let $M : L$ be a splitting field extension for f (where $M \subseteq \overline{K}$). Thus $M : K$ is a splitting field extension for f, so $M : K$ is a normal extension and $M = K(\alpha_1, \ldots, \alpha_n, \ldots, \alpha_r)$ where

$$f = \prod_{i=1}^{r} (t - \alpha_i).$$

Suppose $N \subseteq M$ so that $L \subseteq N$ and $N : K$ is a normal extension. Thus for $1 \leq i \leq n$, $m_{\alpha_i}(K)$ is an irreducible polynomial with a root in L; since $L \subseteq N$; $m_{\alpha_i}(K)$ splits over N. Consequently f splits over N, so $\alpha_1, \ldots, \alpha_n, \ldots, \alpha_r \in N$. Thus $M \subseteq N$, and so $M = N$. Hence M is a normal closure for $L : K$. (As an exercise, one shows that $[M : K] < \infty$.)

Now suppose $L : K$ is an infinite algebraic extension with $K \subseteq L$. Take $A \subseteq L$ so that $L = K(A)$, and set $S = \{m_\alpha(K) : \ \alpha \in A \ \}$. Take $M \subseteq \overline{K}$ so that $M : K$ is a splitting field extension for S. Then $L \subseteq M$ and $M : K$ is a normal extension. Then arguing as above, M is a normal closure of $L : K$. □

Remark. One can show that if M, N are normal closures of $L : K$, then $M : L$ and $N : L$ are isomorphic extensions. Also, in many proofs, one can replace an algebraic closure of a field K by a normal closure of a finite extension $L : K$.

Proposition 6.6. *Suppose $M : K$ is a normal extension.*

(a) *For any $\sigma \in Gal(M : K)$ and $\alpha \in M$, we have $m_{\sigma(\alpha)}(K) = m_\alpha(K)$.*
(b) *For $\alpha, \beta \in M$ with $m_\alpha(K) = m_\beta(K)$, there is some $\tau \in Gal(M : K)$ so that $\tau(\alpha) = \beta$.*

Proof. Assume $K \subseteq M$.

(a) Take $\sigma \in Gal(M : K)$ and $\alpha \in M$. Thus with $g = m_\alpha(K)$,

$$0 = \sigma(g(\alpha)) = g(\sigma(\alpha)).$$

Thus $m_{\sigma(\alpha)}(K) = g = m_\alpha(K)$.

(b) Suppose $\alpha, \beta \in M$ so that $m_\alpha(K) = m_\beta(K)$. Thus by Theorem 3.2, there is a K-isomorphism $\sigma : K(\alpha) \to K(\beta)$ so that $\sigma(\alpha) = \beta$. If $[M : K] < \infty$ then we can repeatedly apply Theorem 3.2 to inductively construct a homomorphism $\tau : M \to \overline{K}$ that extends σ. Whether or not $[M : K] < \infty$, by Theorem 4.5 such a homomorphism τ exists. By Proposition 6.1, $\tau(M) = M$, so $\tau \in Gal(M : K)$. □

Definition. Let K_1, K_2 be fields contained in some field L. We let K_1K_2 denote the smallest subfield of L containing both K_1 and K_2, and we call K_1K_2 the compositum of K_1 and K_2 in L.

Remark. Suppose that $E : K$ and $F : K$ are extensions with E, F, K contained in a field L, and that $E = K(A)$ for some set A contained in E, $F = K(B)$ for some set B contained in F. Then EF must contain K, A, B and hence must contain $K(A \cup B)$. On the other hand, $K(A \cup B)$ contains $E = K(A)$ and $F = K(B)$. Hence $EF = K(A \cup B)$.

Similarly, if $E : K$ is an algebraic extension then

For instance, $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

As an exercise, one shows the following.

Proposition 6.7. *Suppose $E : K$ and $F : K$ are finite extensions so that K, E, F are contained in a field L. Then $EF : K$ is a finite extension. Hence with M a normal closure of $EF : K$, we have that $M : K$ is a finite extension.*

Theorem 6.8. *Let $E : K$ and $F : K$ be finite extensions so that K, E, F are contained in a field L.*

(a) *Suppose that $E : K$ is normal. Then $EF : F$ is normal.*
(b) *Suppose that $E : K$ and $F : K$ are normal. Then $EF : K$ and $E \cap F : K$ are normal.*

Proof. (a) Suppose $E : K$ is normal. Thus, since $E : K$ is finite, $E : K$ is a splitting field extension for some $g \in K[t] \smallsetminus K$ [notice that if $E = K$, we can take $g = t - 1$]. With $\alpha_1, \ldots, \alpha_r \in E$ the roots of g, we have

$$E = K(\alpha_1, \ldots, \alpha_r).$$

We have that $F(\alpha_1, \ldots, \alpha_r)$ is a field containing E and F, and any subfield of this field that contains both E and F necessarily contains $\alpha_1, \ldots, \alpha_r$ and thus contains $F(\alpha_1, \ldots, \alpha_r)$. Hence we must have that $EF = F(\alpha_1, \ldots, \alpha_r)$. So $EF : F$ is a splitting field extension for g. Thus $EF : F$ is a normal extension.

(b) Suppose $E : K$ and $F : K$ are normal extensions. Thus $E : K$ is a splitting field extension for some $g \in K[t] \smallsetminus K$, and $E : K$ is a splitting field extension for some $h \in K[t] \smallsetminus K$. Let

$$A = \{\alpha \in E : \ \alpha \text{ is a root of } g \ \}, \ B = \{\beta \in F : \ \beta \text{ is a root of } h \ \}.$$

Thus $E = K(A)$, $F = K(B)$, and we have $EF = K(A \cup B)$. So $EF : K$ is a splitting field extension for gh. Hence $EF : K$ is normal.

(That $E \cap F : K$ is normal is left as an exercise.) □

As an exercise, one can explore whether the above theorem can be extended to infinite extensions $E : K$, $F : K$.

Example. Set $\alpha = \sqrt[3]{2} \in \mathbb{R}_+$ and $i = \sqrt{-1} \in \mathbb{C}$. $\mathbb{Q}(i) : \mathbb{Q}$ is a normal extension (as it is the splitting field for $m_i(\mathbb{Q}) = t^2 + 1$), but $\mathbb{Q}(\alpha) : \mathbb{Q}$ is not a normal extension extension (as $m_\alpha(\mathbb{Q}) = t^3 - 2$ does not split over $\mathbb{Q}(\alpha)$). $\mathbb{Q}(i)\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha)$ is a normal extension (as it is the splitting field extension

for t^2+1), but $\mathbb{Q}(i)\mathbb{Q}(\alpha):\mathbb{Q}$ is not a normal extension (as t^3-2 does not split over $\mathbb{Q}(i)\mathbb{Q}(\alpha)$).

7. Separability

Definitions. We say an irreducible polynomial $f \in K[t]$ is separable over K if has no repeated (equivalently, no multiple) roots, meaning that $f = \lambda \prod_{i=1}^{d}(t-\alpha_i)$ where $\alpha_1, \ldots, \alpha_d \in \overline{K}$ are distinct (here $\overline{K}$ denotes an algebraic closure of K). We say a nonzero polynomial $f \in K[t]$ is separable over K if its irreducible factors in $K[t]$ are separable over K. With $L:K$ a field extension, we say $\alpha \in L$ is separable over K if α is algebraic over K and $m_\alpha(K)$ is separable. We say an algebraic extension $L:K$ is a separable extension if every $\alpha \in L$ is separable over K. (Note that if $L:K$ is a separable extension then so is $M:K$.)

Remark. Some texts define a polynomial to be separable if it has no multiple roots in an algebraic closure. Also, some texts define a "separability degree" $[L:K]_s$ of an extension $L:K$, and prove that $L:K$ is separable if and only if $[L:K]_s = [L:K]$.

Example. We show that not every irreducible polynomial over a field K is separable over K: Let p be a prime integer, and let $K = \mathbb{F}_p(y)$, where $\mathbb{F}_p$ denotes the field with p elements and y is an indeterminate over $\mathbb{F}_p$ (so y is transcendental over $\mathbb{F}_p$). Set $f = t^p - y \in K[t]$. Let $\alpha \in \overline{K}$ be a root of f. (So $\alpha^p = y$.) We now show that f is irreducible over K. $\mathbb{F}_p(y)$ is the field of fractions of $\mathbb{F}_p[y]$, and the units in $\mathbb{F}_p[y]$ are the non-zero elements of $\mathbb{F}_p$. So y is not a unit in $\mathbb{F}_p[y]$. Suppose $y = gh$ where $g, h \in \mathbb{F}_p[y]$; then

$$1 = \deg y = \deg(gh) = \deg g + \deg h,$$

so either $\deg g = 0$ or $\deg h = 0$, and hence either g or h is a unit in $\mathbb{F}_p[y]$. So y is irreducible in $\mathbb{F}_p[y]$. Since $t^p - y$ is primitive in $\mathbb{F}_p[y]$, by Eisenstein's criterion we have that $f = t^p - y$ is irreducible over $\mathbb{F}_p[y]$, and hence by Gauss's Lemma f is irreducible over $\mathbb{F}_p(y) = K$. However, using that $\mathrm{char} K = p$ and that p divides the binomial coefficients $\binom{p}{k}$ for $1 \le k < p$, we have that

$$(t-\alpha)^p = t^p + (-1)^p \alpha^p = t^p - y.$$

(Recall that when $p = 2$, $-y = y$.) Thus α is the only root of f, even though f is irreducible over K with $\deg f > 1$.

Proposition 7.1. *Suppose $L:M:K$ is an algebraic tower of fields (so $L:M$, $M:K$ are algebraic, and hence $L:K$ is algebraic). Assume that $K \subseteq L \subseteq M \subseteq \overline{K}$, and suppose that $f \in K[t] \smallsetminus K$ so that f is separable over K. If $g \in M[t] \smallsetminus M$ so that $g|f$ then g is separable over M. Thus if $\alpha \in L$ is separable over K then α is separable over M, and if $L:K$ is separable then so is $L:M$.*

Proof. Suppose that $g \in M[t]$ so that $g|f$, and suppose that $g_0 \in M[t]$ is a factor of g that is irreducible over M. So $g_0|f$, and hence by Proposition 4.10, g_0 divides a factor f_0 of f that is irreducible over K. Thus $f_0 = g_0 h_0$ for some $h_0 \in M[t]$. Since f_0 has $\deg f_0$ distinct roots in $\overline{K}$ and $\deg f_0 = \deg g_0 + \deg h_0$, g_0 must have $\deg g_0$ distinct roots in $\overline{K}$ (recall that $\overline{K}[t]$ is a UFD). As this holds for all factors of g that are irreducible over M, g is separable over M.

Now suppose that $\alpha \in L$ is separable over K. Thus α is algebraic over K, and $m_\alpha(K)$ is separable over K. Since $m_\alpha(M)|m_\alpha(K)$, we have that $m_\alpha(M)$ is separable over M, and hence α is separable over M. Hence if $L : K$ is separable, then so is $L : M$. □

As an exercise, one proves the following.

Proposition 7.2. *Suppose $L : M : K$ is an algebraic field extension. For $\alpha \in L$ and $\sigma : M \to \overline{M}$ a homomorphism, $\sigma(m_\alpha(M))$ is separable over $\sigma(M)$ if and only if $m_\alpha(M)$ is separable over M.*

Theorem 7.3. *Suppose $L : K$ is a finite extension with $K \subseteq L \subseteq \overline{K}$, and $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in L$. Set $K_0 = K$, and for $1 \leq i \leq n$, set $K_i = K_{i-1}(\alpha_i)$. Let $\sigma_0 : K \to \overline{K}$ be the inclusion map. If α_i is separable over K_{i-1} for all i, $1 \leq i \leq n$, then there are $[L : K]$ ways to extend σ_0 to a homomorphism $\tau : L \to \overline{K}$. If α_i is not separable over K_{i-1} for some i, $1 \leq i \leq n$, then there are fewer than $[L : K]$ ways to extend σ_0 to a homomorphism $\tau : L \to \overline{K}$.*

Proof. Suppose $\tau : L \to \overline{K}$ is a homomorphism extending σ_0. Then with $\sigma_i = \tau|_{K_i}$, we have that $\sigma_i : K_i \to \overline{K}$ is a homomorphism extending σ_{i-1}. So each homomorphism $\tau : L \to \overline{K}$ corresponds to a sequence of homomorphisms $\sigma_1, \ldots, \sigma_n$ where $\sigma_n = \tau$ and for each i, $1 \leq i \leq n$, $\sigma_i : K_i \to \overline{K}$ extends σ_{i-1}.

Suppose that $1 \leq j \leq n$ and for $1 \leq i < j$, we have homomorphisms $\sigma_i : K_i \to \overline{K}$ so that σ_i extends σ_{i-1}. By Corollary 3.3, the number of ways to extend σ_{j-1} to a homomorphism $\sigma_j : K_j \to \overline{K}$ is the number of (distinct) roots of $\sigma_{j-1}(m_{\alpha_j}(K_{j-1}))$ that lie in $\overline{K}$, and by Corollary 4.6, this number is the number of (distinct) roots of $m_{\alpha_j}(K_{j-1})$ that lie in $\overline{K}$ (recall that by Proposition 4.9, since $K \subseteq K_{j-1}$ and $K_{j-1} : K$ is algebraic, we have $\overline{K} = \overline{K}_{j-1}$). Thus the number of ways to extend σ_{j-1} to σ_j is $\deg m_{\alpha_j}(K_{j-1}) = [K_j : K_{j-1}]$ if α_j is separable over K_{j-1}, and it is few than σ_j is $\deg m_{\alpha_j}(K_{j-1}) = [K_j : K_{j-1}]$ if α_j is not separable over K_{j-1}. The result now follows. □

Theorem 7.4. *Suppose $L : K$ is a finite extension with $L = K(\alpha_1, \ldots, \alpha_n)$. Set $K_0 = K$ and for $1 \leq i \leq n$, inductively define K_i by $K_i = K_{i-1}(\alpha_i)$. The following are equivalent:*

(i) *For all $1 \leq i \leq n$, α_i is separable over K_{i-1}.*
(ii) *For all $1 \leq i \leq n$, α_i is separable over K.*
(iii) *$L : K$ is a separable extension.*

Proof. Suppose that $K \subseteq L \subseteq \overline{K}$ where $\overline{K}$ is an algebraic closure of K (and hence of L).

To show (i) implies (iii): Assume that (i) holds. Thus by Theorem 7.3, there are $[L : K]$ K-homomorphisms $\tau : L \to \overline{K}$. Choose $\beta_1 \in L$. Since $[L : K] < \infty$, we know that β_1 is algebraic over K and $L = K(\beta_1, \beta_2, \ldots, \beta_m)$ for some $\beta_2, \ldots, \beta_m \in L$. Set $K'_0 = K$, and for $1 \leq j \leq m$, set $K'_j = K(\beta_1, \ldots, \beta_j) = K'_{j-1}(\beta_j)$. Thus β_1 must be algebraic over K, else by Theorem 7.3 we would have that there are fewer than $[L : K]$ K-homomorphisms $\tau : L \to \overline{K}$ }. This argument holds for all $\beta_1 \in L$, so $L : K$ is separable.

To show (iii) implies (ii): This follows from the definition of $L : K$ being a separable extension.

To show (ii) implies (i): This follows from Proposition 7.1. □

An immediate consequence of Theorems 7.3 and 7.4 is the following.

Corollary 7.5. *Suppose $L : K$ is a finite extension. If $L : K$ is a separable extension then there are $[L : K]$ K-homomorphisms $\sigma : L \to \overline{K}$. If $L : K$ is not separable then there are fewer than $[L : K]$ K-homomorphisms $\sigma : L \to \overline{K}$.*

Corollary 7.6. *Suppose that $f \in K[t] \setminus K$ and that $L : K$ is a splitting field extension for f. Then $L : K$ is a separable extension if and only if f is separable over K. More generally, suppose $L : K$ is a splitting field extension for $S \subseteq K[t] \setminus K$. Then $L : K$ is a separable extension if and only if each $f \in S$ is separable over K.*

Proof. Assume that $K \subseteq L$. We first consider that case that $L : K$ is a splitting field extension for $f \in K[t] \setminus K$.

Suppose first that f is separable over K. Let $\alpha_1, \ldots, \alpha_n \in L$ be the roots of f; thus $L = K(\alpha_1, \ldots, \alpha_n)$. For each i, $1 \leq i \leq n$, $m_{\alpha_i}(K)$ is a factor of f that is irreducible over K; since f is separable over K, so is $m_{\alpha_i}(K)$. Hence for each i, α_i is separable over K. Thus by Theorem 7.4 ((ii) if and only if (iii)), we have that $L : K$ is a separable extension.

Now suppose $L : K$ is a separable extension that is a splitting field extension for f. Every root of f is algebraic over K, and since $L : K$ is separable, this means that every root of f is separable over K. Hence f is separable over K.

Now suppose that $L : K$ is a splitting field extension for $S \subseteq K[t] \setminus K$, and that each element of S is separable over K. Take $\alpha \in L$. Thus by Proposition 1.9, $\alpha \in D$ where D is some finite subset of

$$A = \{\beta \in L : \ g(\beta) = 0 \text{ for some } g \in S \ \}.$$

For each $\beta \in D$, choose $g_\beta \in S$ so that β is a root of g_β. Set $h = \prod_{\beta \in D} g_\beta$, and let $M : K$ be a splitting field extension for h; assume that $K \subseteq M \subseteq L$. Since each g_β is separable over K ($\beta \in D$), h is separable over K. Thus by the first part of this Corollary, $M : K$ is separable. Since $\alpha \in K(D) \subseteq M$, we have that α is separable over K. As this argument holds for all $\alpha \in L$, we have that $L : K$ is separable.

Conversely, suppose $L : K$ is a splitting field extension for $S \subseteq K[t] \setminus K$ and $L : K$ is a separable extension. Thus for any $f \in S$, the roots of f are separable over K, and hence f is separable over K. □

We have already seen that if $L : K$ is separable then so are $L : M$ and $M : K$. To prove the converse, it is convenient to have the Primitive

Element Theorem, which is proved in section 9. Hence the part of the following theorem is proved as an exercise for section 9.

Theorem 7.7. *Suppose that $L : M : K$ is an algebraic tower of fields. $L : K$ is separable if and only if $L : M$ and $M : K$ are both separable.*

One also proves the following as an exercise.

Theorem 7.8. *Suppose that $E : K$ and $F : K$ are finite extensions with $E, F \subseteq L$ where L is a field.*

(a) *When $E : K$ is separable, so is $EF : F$.*
(b) *When $E : K$ and $F : K$ are both separable, so are $EF : K$ and $(E \cap F) : K$.*

8. Inseparable polynomials, differentiation, and the Frobenius map

Definition. We say a polynomial $f \in K[t]$ is inseparable over K if f is not separable over K, meaning that f has an irreducible factor $g \in K[t]$ so that g has fewer than $\deg g$ (distinct) roots in $\overline{K}$.

Definition. We define the derivative operator $D : K[t] \to K[t]$ by

$$D\left(\sum_{k=0}^{n} a_k t^k\right) = \sum_{k=1}^{n} k a_k t^{k-1}$$

where $2a = a + a$, $3a = a + a + a$, and so on.

One easily verifies that with $\alpha \in K$ and $f, g \in K[t]$, $D(f+g) = Df + Dg$, $D(\alpha f) = \alpha(Df)$, and for $m, n \in \mathbb{Z}_+$,

$$D(t^m t^n) = (m+n)t^{m+n-1} = (Dt^m)t^n + t^m(Dt^n).$$

Consequently

$$D(fg) = (Df)g + f(Dg).$$

As an exercise, one proves the following.

Theorem 8.1. *Let $f \in K[t]$, $f \neq 0$, and let $L : K$ be a splitting field extension for f. Assume that $K \subseteq L$. The following are equivalent:*

(i) *f is inseparable over K.*
(ii) *There is some $\alpha \in L$ so that $f(\alpha) = 0 = (Df)(\alpha)$.*
(iii) *There is some $g \in K[t]$ so that $\deg g \geq 1$ and g divides both f and Df.*

Theorem 8.2. *Suppose that $f \in K[t]$ is irreducible over K. Then f is inseparable over K if and only if $charK = p > 0$, and $f \in K[t^p]$, meaning that*

$$f = a_0 + a_1 t^p + a_2 t^{2p} + \cdots + a_n t^{np},$$

where $a_0, \ldots, a_n \in K$.

Proof. Suppose that $f \in K[t]$ is irreducible over K.

Suppose first that f is inseparable over K; write

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n$$

where $a_0, \ldots, a_n \in K$. Thus there is some $g \in K[t]$ so that $\deg g \geq 1$ and g divides both f and Df. So $f = gh$ for some $h \in K[t]$. Since f is irreducbile and g is not a unit, h must be a unit (i.e. $h \in K^\times$). Since g divides Df, we must have that f divides Df. But either $Df = 0$ or $\deg Df < \deg f$. As f does not divide any nonzero polynomial of degree less than $\deg f$, we must have that $Df = 0$. Hence

$$0 = Df = a_1 + 2a_2 t + \cdots + n a_n t^{n-1}.$$

Thus we must have that $\mathrm{char} K = p > 0$, and for $1 \leq r \leq n$, we must have $r a_r = 0$, so either p divides r or $a_r = 0$. Hence

$$f = b_0 + b_1 t^p + b_2 t^{2p} + \cdots + b_m p^{mp}$$

for some $m \in \mathbb{Z}_+$ and some $b_0, \ldots, b_m \in K$. Thus $f \in K[t^p]$.

Now suppose that $\mathrm{char} K = p > 0$ and $f \in K[t^p]$. Then $Df = 0$, and hence by Theorem 8.1, f is inseparable over K. □

Corollary 8.3. *Suppose that $\mathrm{char} K = 0$. Then all polynomials in $K[t]$ are separable over K.*

Definition. Suppose $\mathrm{char} K = p > 0$. Define the Frobenius map $\phi : K \to K$ by $\phi(\alpha) = \alpha^p$.

Theorem 8.4. *Suppose $\mathrm{char} K = p > 0$, and let F be the prime subfield of K. Let ϕ denote the Frobenius map from K into K. Then ϕ is an injective homomorphism, and*

$$\{\alpha \in K : \ \phi(\alpha) = \alpha \ \} = F.$$

Proof. Take $\alpha, \beta \in K$. Clearly $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$, and $\phi(1) = 1$. Also,

$$\phi(\alpha + \beta) = \sum_{k=0}^{p} \binom{p}{k} \alpha^k \beta^{p-k}.$$

For $0 < k < p$, we know p divides $\binom{p}{k}$, so

$$\phi(\alpha + \beta) = \alpha^p + \beta^p = \phi(\alpha) + \phi(\beta).$$

Hence ϕ is a homomorphism, which is necessarily injective since K is a field.

We have that $F = \{c \cdot 1_K : \ c \in \mathbb{Z}, \ 1 \leq c \leq p \ \}$, and

$$\phi(c \cdot 1_K) = c \cdot \phi(1_K) = c \cdot 1_K.$$

Thus $F \subseteq \{\alpha \in K : \ \phi(\alpha) = \alpha \ \}$. On the other hand, every element of $\{\alpha \in K : \ \phi(\alpha) = \alpha \ \}$ is a root of the polynomial $t^p - t$, and this polynomial has at most p roots in K. Hence $F = \{\alpha \in K : \ \phi(\alpha) = \alpha \ \}$. □

One proves the following two corollaries as exercises.

Corollary 8.5. *Suppose $\mathrm{char} K = p > 0$ and K is algebraic over its prime subfield. Then the Frobenius map is an automorphism of K.*

Corollary 8.6. *Suppose $charK = p > 0$ and K is algebraic over its prime subfield. Then all polynomials in $K[t]$ are separable over K.*

Theorem 8.7. *Suppose that $charK = p > 0$ and that*

$$f(t) = g(t^p) = a_0 + a_1 t^p + a_2 t^{2p} + \cdots + a_{n-1} t^{(n-1)p} + t^{np}$$

is a nonconstant monic polynomial over K. Then $f(t)$ is irreducible in $K[t]$ if and only if $g(t)$ is irreducible in $K[t]$ and not all the coefficients a_i are pth powers in K.

Proof. We prove the contrapositive.

First suppose that g is reducible in $K[t]$. Thus $g = g_1 g_2$ for some $g_1, g_2 \in K[t]$ with $\deg g_1 \geq 1$, $\deg g_2 \geq 1$. Hence $f = g(t^p) = g_1(t^p) g_2(t^p)$, and $\deg g_1(t^p) \geq 1$, $\deg g_2(t^p) \geq 1$. So when $g(t)$ is reducible, so is $f(t)$. Equivalently, when $f(t)$ is irreducible, so is $g(t)$.

Suppose that for $1 \leq i \leq n$, $a_i = b_i^p$ for some $b_i \in K$. Then (using the Binomial Theorem and the fact that $\mathrm{char}K = p > 0$),

$$f = (b_0 + b_1 t + b_2 t^2 + \cdots + b_{n-1} t^{n-1} + t^n)^p.$$

So if every coefficient a_i is a pth power, then f is reducible. Equivalently, if f is irreducible then not every coefficient a_i is a pth power.

Now suppose that f is reducible. Thus $f = f_1^{m_1} \cdots f_r^{m_r}$ where $f_1, \ldots, f_r$ are distinct monic irreducible polynomials over K and $m_1, \ldots, m_r \in \mathbb{Z}_+$. Suppose first that $r > 1$; set $h_1 = f_1^{m_1}$, $h_2 = f/h_1$. Thus $\mathrm{hcf}(h_1, h_2) = 1$, so the ideal generated by h_1, h_2 is the entire ring $K[t]$. Hence there are $\lambda_1, \lambda_2 \in K[t]$ so that $\lambda_1 h_1 + \lambda_2 h_2 = 1$. But since $f(t) = g(t^p)$, we know that $Df = 0$, so

$$(Dh_1)h_2 + h_1(Dh_2) = 0.$$

Hence

$$Dh_1 = \lambda_1 h_1 (Dh_1) + \lambda_2 h_2 (Dh_1) = \lambda_1 h_1 (Dh_1) - \lambda_2 h_1 (Dh_2),$$

and so h_1 divides Dh_1. So Dh_1 must be 0. A similar argument shows that Dh_2 must be 0. So

$$h_1 = c_0 + c_1 t^p + \cdots + c_s t^{sp}, \ h_2 = d_0 + d_1 t^p + \cdots + d_k t^{kp};$$

note that $s, k \geq 1$. Hence $g(t) = (c_0 + c_1 t + \cdots + c_s t^s)(d_0 + d_1 t + \cdots + d_k t^k)$, so $g(t)$ is reducible in $K[t]$.

Now suppose $r = 1$, so $f = f_1^m$ where f_1 is irreducible over K, $m = m_1$, and necessarily $m > 1$. If $p|m$ then $f = h^p$ for some $h = c_0 + c_1 t + \cdots + c_s t^s \in K[t]$, and so

$$f = h^p = c_0^p + c_1^p t^p + \cdots + c_s^p t^{sp}.$$

If $p \nmid m$ then

$$0 = Df = m(Df_1) f_1^{m-1},$$

so $Df_1 = 0$; hence

$$f_1(t) = d_0 + d_1 t^p + \cdots + d_k t^{kp} = g_1(t^p),$$

and $g = g_1^m$, which is reducible. □

9. The Primitive Element Theorem

Definition. Suppose $L : K$ is a field extension relative to the embedding $\varphi : K \to L$. We say $L : K$ is a simple extension of there is some $\gamma \in L$ so that $L = \varphi(K)(\gamma)$.

Theorem 9.1. *(The Primitive Element Theorem) Let $L : K$ be a finite, separable extension (hence $L : K$ is an algebraic extension). Assume $K \subseteq L$. Then $L : K$ is a simple extension.*

Proof. Assume $L \subseteq \overline{K}$ where $\overline{K}$ is an algebraic closure of K.

Suppose first that K is finite. Then L is finite (with $|L| = |K|^{[L:K]}$). Thus $L^\times = L \smallsetminus \{0\}$ is cyclic (as a multiplicative group), with some generator $\gamma \in L^\times$. Hence $L = K(\gamma)$.

Now suppose K is infinite. Take $\alpha_1 \in L$. If $L = K(\alpha_1)$ then we are done; so suppose not. Then there is some $\alpha_2 \in L \smallsetminus K(\alpha_1)$. Let $r = [K(\alpha_1, \alpha_2) : K]$. Since $L : K$ is separable, we know $K(\alpha_1, \alpha_2) : K$ is separable, and hence by Theorem 7.3 there are r distinct K-homomorphisms $\varphi_1, \ldots, \varphi_r : K(\alpha_1, \alpha_2) \to \overline{K}$. (Recall that $m_{\alpha_2}(K)$ is separable over K, hence $m_{\alpha_2}(K(\alpha_1))$ is separable over $K(\alpha_1)$.) Set

$$f = \prod_{\substack{1 \le i,j \le r \\ i \ne j}} \Big(\big(\varphi_i(\alpha_1) - \varphi_j(\alpha_1)\big) + \big(\varphi_i(\alpha_2) - \varphi_j(\alpha_2)\big)t \Big).$$

One checks that $f \ne 0$, and that there is some $\delta \in K$ so that $f(\delta) \ne 0$. Set $\gamma = \alpha_1 + \alpha_2\delta$. One checks that for $i \ne j$, we have $\varphi_i(\gamma) \ne \varphi_j(\gamma)$. Thus $\varphi_1, \ldots, \varphi_r$ must restrict to distinct K-homomorphisms from $K(\gamma)$ into $\overline{K}$. Hence the number of distinct roots of $m_\gamma(K)$ in $\overline{K}$ must be at least r. So $m_\gamma(K)$ has at least r roots in $\overline{K}$, and hence $\deg m_\gamma(K) \ge r$. This means that $[K(\gamma) : K] \ge r$. Since $K(\gamma) \subseteq K(\alpha_1, \alpha_2)$, the Tower Law shows that we have

$$r \le [K(\gamma) : K] \le [K(\alpha_1, \alpha_2) : K] = r,$$

and thus $K(\gamma)$ must equal $K(\alpha_1, \alpha_2)$.

Suppose $K(\gamma) \ne L$. We know $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in L$. Hence induction on n shows that $L : K$ is a simple extension. □

As an exercise, one proves the following.

Corollary 9.2. *Suppose that $L : K$ is an algebraic, separable extension, and suppose that for every $\alpha \in L$, $m_\alpha(K)$ has degree at most n over K. Then $[L : K] \le n$.*

Example. Let p be a prime, $\mathbb{F}_p$ the finite field with p elements, and let x, y be indeterminates (so x, y are transcendental over $\mathbb{F}_p$). Set $K = \mathbb{F}_p(x^p, y^p)$, $L = \mathbb{F}_p(x, y)$. Thus $L : K$ is an algebraic extension that is not simple. Further, $L : K$ is not a separable extension, as $t - x^p$, $t - y^p$ are not separable over K.

10. Fixed fields and Galois extensions

Throughout, assume L, K are fields.

Definition. Let $L : K$ be an extension. For G a subgroup of $Aut(L)$, we define the fixed field of G to be

$$Fix_L(G) = \{\alpha \in L : \ \forall \sigma \in G, \ \sigma(\alpha) = \alpha \ \}.$$

As exercises, one proves the following.

Proposition 10.1. *Let K, M, L be fields so that $K \subseteq L$ and $M \subseteq L$. Suppose G and H are subgroups of $Aut(L)$. One has the following.*

(a) *If $K \subseteq M$ then $Gal(L : K) \supseteq Gal(L : M)$.*
(b) *If G is a subgroup of H, then $Fix_L(G) \supseteq Fix_L(H)$.*
(c) *$K \subseteq Fix_L(Gal(L : K))$.*
(d) *$G \subseteq Gal(L : Fix_L(G))$.*
(e) *$Gal(L : K) = Gal(L : Fix_L(Gal(L : K)))$.*
(f) *$Fix_L(G) = Fix_L(Gal(L : Fix_L(G)))$.*

Definition. With $L : K$ a field extension, we say $L : K$ is a Galois extension if it is an extension that is normal and separable.

Theorem 10.2. *Suppose that L is a field and G is a finite subgroup of $Aut(L)$; let $K = Fix_L(G)$. Then $L : K$ is a finite Galois extension (meaning that $L : K$ is a Galois extension with $[L : K] < \infty$), $[L : K] = |Gal(L : K)|$, and $G = Gal(L : K)$.*

Proof. Take $\alpha \in L$ ($\alpha \neq 0$). Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$ be the distinct elements in the G-orbit of α (so $r \leq |G|$ and $\alpha_1, \ldots, \alpha_r \in L$). Set

$$f_\alpha = (t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_r).$$

For each $\sigma \in G$, we know σ is injective, and for each i, $\sigma(\alpha_i)$ is in the G-orbit of α; thus σ must permute $\alpha_1, \alpha_2, \ldots, \alpha_r$. Hence f_α is fixed by each $\sigma \in G$, so $f_\alpha \in K[t]$. Also, by construction, f is separable over K, and f splits over L. Since α is a root of $f_\alpha \in K[t]$, α is algebraic over K and $m_\alpha(K)$ must divide f_α; hence $\deg m_\alpha(K) \leq \deg f_\alpha \leq |G|$, $m_\alpha(K)$ is separable over K and $m_\alpha(K)$ splits over L. As this argument holds for every $\alpha \in L$, $L : K$ is an algebriac extension. Also, for every $\alpha \in L$, we have shown that $m_\alpha(K)$ is separable over K and splits over L; thus $L : K$ is a separable, normal extension, and so it is a Galois extension. Further, since $\deg m_\alpha(K) \leq |G|$ for every $\alpha \in L$, by Corollary 9.2 we have that $[L : K] \leq |G| < \infty$.

Since $L : K$ is Galois, we know $[L : K] = |Gal(L : K)|$.

Now, since $L : K$ is a finite, separable extension, by the Primitive Element Theorem there is some $\gamma \in L$ so that $L = K(\gamma)$. So $[L : K] = \deg m_\gamma(K) \leq \deg f_\gamma \leq |G|$ (where the last equality holds since there are at most $|G|$ distinct elements in the G-orbit of γ). But we also know that $G \subseteq Gal(L : K)$, so $|G| \leq |Gal(L : K)| = [L : K]$. Hence $|G| = |Gal(L : K)|$ and so (remembering that $G \subseteq Gal(L : K)$) we have $G = Gal(L : K)$. □

Theorem 10.3. *Suppose $L : K$ is an algebraic extension. The following are equivalent.*

(i) $L : K$ *is a Galois extension.*
(ii) $L : K$ *is a splitting field extension for a set* $S \subseteq K[t] \setminus K$ *so that for all* $f \in S$, f *is separable over* K.
(iii) $K = Fix_L(Gal(L : K))$.

Proof. Since $L : K$ is algebraic, we can assume $K \subseteq L \subseteq \overline{K}$.

To show (i) implies (ii): Suppose $L : K$ is Galois. Then by Proposition 6.2, $L : K$ is a splitting field extension for some $S \subseteq K[t]$. Take $f \in S$, and suppose $g \in K[t]$ is a monic factor of f with g irreducible. Thus g splits over L, and since g is monic, $g = m_\alpha(K)$ for some $\alpha \in L$. Since $L : K$ is a separable extension, $g = m_\alpha(K)$ is separable over K. As this holds for all monic factors of f that are irreducible over K, it holds that every factor of f that is irreducible over K is separable over K. Hence f is separable over K.

To show (ii) implies (iii): Suppose $L : K$ is a splitting field extension for a set $S \subseteq K[t] \setminus K$ of polynomials that are separable over K. Set $G = Gal(L : K)$. So $K \subseteq Fix_L(G)$. Take $\alpha \in Fix_L(G)$. Let $\beta \in L$ be a root of $m_\alpha(K)$. We know there is some $\varphi \in G$ so that $\varphi(\alpha) = \beta$. But $\alpha \in Fix_L(G)$, so $\varphi(\alpha) = \alpha$. Since $L : K$ is normal, by Theorem 6.2, $m_\alpha(K)$ splits over L; thus α is the only root of $m_\alpha(K)$. Hence $m_\alpha(K) = (t-\alpha)^r$ for some $r \in \mathbb{Z}_+$. But $L : K$ is separable, so $m_\alpha(K)$ has no multiple roots. Thus $r = 1$ and $\alpha \in K$. Hence $Fix_L(G) \subseteq K$, and consequently $Fix_L(G) = K$.

To show (iii) implies (i): Now suppose that $K = Fix_L(Gal(L : K))$. Let $G = Gal(L : K)$. For $\alpha \in L$, let $\alpha, \alpha_2, \ldots, \alpha_r$ be the distinct elements in the G-orbit of α. Set

$$f_\alpha = (t - \alpha)(t - \alpha_2) \cdots (t - \alpha_r).$$

Then f_α is fixed by G (since G permutes the roots of f_α), so $f_\alpha \in Fix_L(G)[t] = K[t]$. By construction, f_α is separable over K. Since $f_\alpha \in K[t]$ and α is a root of f_α, we know that $m_\alpha(K)$ divides f_α, and hence $m_\alpha(K)$ is separable over K. [In fact, $m_\alpha(K) = f_\alpha$, since for $i = 2, \ldots, r$, there is some $\varphi \in G$ so that $\varphi(\alpha) = \alpha_i$, so α_i is a root of $m_{\alpha_i}(K)$ for $i = 2, \ldots, r$.] This argument holds for all $\alpha \in L$, so $L : K$ is separable. Therefore $S = \{ m_\alpha(K) : \ \alpha \in L \}$ is a set of separable polynomials from $K[t]$, and $L : K$ is a splitting field extension for S. Hence $L : K$ is normal and separable. □

Theorem 10.4. *Suppose* $L : K$ *is a finite extension. Then* $L : K$ *is a Galois extension if and only if* $|Gal(L : K)| = [L : K]$.

Proof. Note that $L : K$ is algebraic since $L : K$ is a finite extension. Assume $K \subseteq L \subseteq \overline{K}$.

Suppose first that $L : K$ is a Galois extension. Choose $\alpha_1, \ldots, \alpha_n \in L$ so that $L = K(\alpha_1, \ldots, \alpha_n)$. Since $L : K$ is separable, each α_i is separable over K, and hence by Corollary 7.4, for $i > 1$, α_i is separable over $K(\alpha_1, \ldots, \alpha_{i-1})$. Then by Corollary 7.5, there are $[L : K]$ K-homomorphisms $\tau : L \to \overline{K}$. Since $L : K$ is normal, by Proposition 6.1 $\tau \in Aut(L)$ and hence $\tau \in Gal(L : K)$. Thus $|Gal(L : K)| \geq [L : K]$. We also know by Theorem 3.5 that $|Gal(L : K)| \leq [L : K]$, so $|Gal(L : K)| = [L : K]$.

Now suppose that $L : K$ is not a Galois extension; so either $L : K$ is not separable or it is not normal. This means that there is some $\alpha \in L$

so that $m_\alpha(K)$ is not separable over K or $m_\alpha(K)$ does not split over L. In either case, L contains fewer than $\deg m_\alpha(K)$ roots of $m_\alpha(K)$. Since $\deg m_\alpha(K) = [K(\alpha) : K]$, by Corollary 3.3, the number of ways to extend the identity map on K to a homomorphism $\sigma : K(\alpha) \to L$ is less than $[K(\alpha) : K]$. By Corollary 3.7, the number of ways to extend such σ to an element of $\tau \in Gal(L : K)$ is at most $[L : K(\alpha)]$. By Corollary 3.6, we can construct every element of $Gal(L : K)$ by first extending the identity map on K to a homomorphism $\sigma : K(\alpha) \to L$, and then extending σ to a homomorphism $\tau : L \to L$. Hence $|Gal(L : K)| < [K(\alpha) : K][L : K(\alpha)] = [L : K]$. □

It is useful to record the following easily obtained result.

Proposition 10.5. *Suppose $L : K$ is a Galois extension. Suppose $L : M : K$ is a tower of field extensions. Then $L : M$ is a Galois extension.*

Proof. By assumption, $L : K$ is a normal, separable extension. So by Proposition 6.3, $L : M$ is a normal extension. By Theorem 7.1, $L : M$ is separable. Hence $L : M$ is Galois. □

11. The main theorems of Galois theory

Throughout, let K and L be fields.

Definition. Suppose $L : K$ is a field extension. For G a subgroup of $Aut(L)$, let $\phi(G) = Fix_L(G)$, and for $L : M : K_0$ a tower of field extensions where $K_0 = \phi(Gal(L : K))$, let $\gamma(M) = Gal(L : M)$.

Theorem 11.1. *(The Fundamental Theorem of Galois Theory) Suppose that $L : K$ is a finite extension, and let $G = Gal(L : K)$. Set $K_0 = \phi(G)$. We have the following.*

(a) *The map ϕ is a bijection from the set of subgroups of G onto the set of fields M intermediate between L and K_0, and γ is the inverse map.*
(b) *Suppose H is a subgroup of G. Then $H \lhd G$ if and only if $\phi(H) : K_0$ is a normal extension.*
(c) *When $H \lhd G$, we have $Gal(\phi(H) : K_0) \simeq G/H$. In particular, if $\sigma \in G$, we has $\sigma|_{\phi(H)} \in Gal(\phi(H) : K_0)$ and the map $\sigma \to \sigma|_{\phi(H)}$ is a homomorphism of G onto $Gal(\phi(H) : K_0)$ with kernel H.*

Proof. Note that since $K \subseteq K_0$ and $[L : K] < \infty$, we have $[L : K_0] < \infty$.

(a) Note that $K \subseteq K_0$, so $[L : K_0] \leq [L : K] < \infty$. By Theorem 10.2, $L : K_0$ is a Galois extension, and hence by Theorem 10.4, $|G| = [L : K_0]$.

Take $H \leq G$; so H is a finite subgroup of $Aut(L)$. Then by Theorem 10.2, $L : \phi(H)$ is a Galois extension and $H = Gal(L : \phi(H))$. Thus we have $H = \gamma\phi(H)$, and hence ϕ is injective and γ is surjective. [Recall that when $g \circ f$ is a bijective map, then f is injective and g is surjective.]

Now suppose M is a field with $K_0 \subseteq M \subseteq L$. Thus $[L : M] < \infty$ since $[L : K_0] < \infty$. By Proposition 10.5, $L : M$ is a Galois extension. Thus by Theorem 10.3, $\phi\gamma(M) = M$. Hence γ is injective and ϕ is surjective. Therefore ϕ and γ are bijective maps and are inverses of each other.

(b) Suppose that $H \lhd G$. As an exercise, one shows that for all $\sigma \in G$, we have $H = \gamma\sigma\phi(H)$, and hence by (a),

$$\phi(H) = \sigma\phi(H).$$

Thus $\phi(H)$ is fixed by all $\sigma \in G$. By Proposition 6.1, for all $\sigma \in G$ we have $\sigma|_{\phi(H)} \in Aut(\phi(H))$. Then, since $L : K_0$ is a finite, normal extension with intermediate field $\phi(H)$, Theorem 6.4 implies that $\phi(H) : K_0$ is normal, as desired.

Now suppose that $\phi(H) : K_0$ is normal. Take $\sigma \in G$. By Theorem 6.4, $\sigma\phi(H) = \phi(H)$. Take $\tau \in H$, $\alpha \in \phi(H)$. Then with $\beta = \sigma(\alpha)$, we have $\beta \in \phi(H)$, and

$$\sigma^{-1}\tau\sigma(\alpha) = \sigma^{-1}\tau(\beta) = \sigma^{-1}(\beta) = \alpha.$$

Hence $\sigma^{-1}\tau\sigma \in Aut(L)$ and $\sigma^{-1}\tau\sigma(\alpha) = \alpha$ for all $\alpha \in \phi(H)$. That is, $\sigma^{-1}\tau\sigma \in Gal(L : \phi(H)) = \gamma\phi(H) = H$. So $H \lhd G$.

(c) Suppose $H \lhd G$. Take $\sigma \in G$. Thus by Theorem 6.4, $\sigma|_{\phi(H)} \in Gal(\phi(H) : K_0)$, and as an exercise one checks that the map $\sigma \mapsto \sigma|_{\phi(H)}$ is a surjective homomorphism from $G = Gal(L : K_0)$ to $Gal(\phi(H) : K_0)$. The kernel of this map is

$$\{\sigma \in G : \ \sigma|_{\phi(H)} = id_{\phi(H)} = Gal(L : \phi(H)) = \gamma\phi(H) = H.$$

Thus by the First Isomorphism Theorem of Group Theory,

$$Gal(L : K_0)/Gal(L : \phi(H)) \simeq Gal(\phi(H) : K_0),$$

completing the proof. □

Notation. Given $f \in K[t]$ and $L : K$ a splitting field extension for f, we use $Gal_K(f)$ to denote $Gal(L : K)$.

Suppose f is irreducible and separable over K. Let $L : K$ be a splitting field extension for f, and assume $K \subseteq L$ (so $L : K$ is a Galois extension). We discuss the general strategy for determining the structure of $Gal_K(f)$. In doing this, we will use Corollary 6.6, which implies that for any $g \in K[t]$ so that g is irreducible over K, $Gal(L : K)$ permutes the roots of g transitively. Let $\alpha_1, \ldots, \alpha_n \in L$ be the roots of f where $n = \deg f$. For $\sigma : L \to L$ a K-homomorphism, we know from Proposition 6.1 that $\sigma \in Aut(L)$, and hence $\sigma \in Gal(L : K)$. For $\sigma \in Gal(L : K)$, we know that $\sigma(\alpha_i\alpha_j) = \sigma(\alpha_i)\sigma(\alpha_j)$ for each i, j $(1 \leq i, j \leq n)$. Also, by Proposition 6.6, we know that $\sigma(\alpha_i)$ is another root of f, and since σ is injective, for all i $(1 \leq i \leq n)$ we have $\sigma(\alpha_i) = \alpha_{\nu(i)}$ where ν is some element of S_n, the permutation group on $\{1, 2, \ldots, n\}$. By checking all relations involved in generating $K(\alpha_1, \ldots, \alpha_n)$, we can check whether a candidate for a K-homomorphism of L is indeed a K-homomorphism of L (as we demonstrate in the following example). Also, since we are assuming that $L : K$ is a Galois extension, we know that there are $|Gal(L : K)| = [L : K]$, so once we find $[L : K]$ K-homomorphisms of L, we know we have all the elements of $Gal(L : K)$.

Example. Let $K = \mathbb{Q}$, $f = t^4 - 2t^2 + 2$. By Eisenstein's Criterion [with $p = 2$], f is irreducible over $\mathbb{Z}$, and then by Gauss' Lemma, f is irreducible over $\mathbb{Q}$. Since char$\mathbb{Q} = 0$, f is separable over $\mathbb{Q}$. We have

$$t^4 - 2t^2 + 2 = (t^2 - 1)^2 + 1,$$

so $f(\alpha) = 0$ if and only if $\alpha^2 - 1 = \pm i$, or equivalently, $\alpha = \pm\sqrt{1 \pm i}$ (here $i = \sqrt{-1}$). [Alternatively, one could first solve for α^2 using the Quadratic Equation.] Set $\xi = \sqrt{1+i}$ and $\xi' = \sqrt{1-i}$. Thus the roots of f are $\pm\xi$, $\pm\xi'$. Hence with $L = \mathbb{Q}(\xi, \xi')$, $L : \mathbb{Q}$ is a splitting field extension for f. Thus $L : \mathbb{Q}$ is a Galois extension and $[L : \mathbb{Q}] = |Gal(L : \mathbb{Q})|$. Also, notice that

$$\mathbb{Q}(\xi, \xi') = \mathbb{Q}(\xi, \sqrt{2}/\xi) = \mathbb{Q}(\xi, \sqrt{2}).$$

We know that $\deg m_\xi(\mathbb{Q}) = 4$, so by the Tower Law, $4|[L : \mathbb{Q}]$. Also, $m_{\sqrt{2}}(\mathbb{Q}(\xi))$ divides $m_{\sqrt{2}}(\mathbb{Q}) = t^2 - 2$, so $[L : \mathbb{Q}(\xi)] \leq 2$. Hence again by the Tower Law, $|Gal(L : \mathbb{Q})| = [L : \mathbb{Q}] = 4$ or 8.

Note that $\xi\xi' = \sqrt{2}$, and $\xi^2 = 1 + i$. So $\sqrt{2}, i, i\sqrt{2} \in L$.

To construct the elements of $G = Gal(L : \mathbb{Q})$, recall that G is transitive on the roots of f, which are $\{\pm\xi, \pm\xi'\}$, and each element of G is a $\mathbb{Q}$-homomorphism that permutes the roots of f. (So for $\sigma \in G$, we have $\sigma(-\xi) = -\sigma(\xi)$, $\sigma(-\xi') = -\sigma(\xi')$, and thus σ is determined by its action on ξ and ξ'.) So we consider the possibilities, as follows.

• $\sigma_1(\xi) = \xi$, $\sigma_1(\xi') = \xi'$ (and so σ_1 is the identity map, implying that $\sigma_1(\sqrt{2}) = \sqrt{2}$ and $\sigma_1(i) = i$).

• $\sigma_2(\xi) = \xi$, $\sigma_2(\xi') = -\xi'$ (and so if σ_2 is indeed a $\mathbb{Q}$-homomorphism, $\sigma_2(\sqrt{2}) = \sigma_2(\xi)\sigma_2(\xi') = -\sqrt{2}$, and $\sigma_2(i) = i$).

• $\sigma_3(\xi) = -\xi$, $\sigma_3(\xi') = \xi'$ (and so if σ_3 is indeed a $\mathbb{Q}$-homomorphism, $\sigma_3(\sqrt{2}) = \sigma_3(\xi)\sigma_3(\xi') = -\sqrt{2}$, and $\sigma_3(i) = i$).

• $\sigma_4(\xi) = -\xi$, $\sigma_4(\xi') = -\xi'$ (and so if σ_4 is indeed a $\mathbb{Q}$-homomorphism, $\sigma_4(\sqrt{2}) = \sqrt{2}$, and $\sigma_4(i) = i$).

• $\sigma_5(\xi) = \xi'$, $\sigma_5(\xi') = \xi$ (and so if σ_5 is indeed a $\mathbb{Q}$-homomorphism, $\sigma_5(\sqrt{2}) = \sqrt{2}$, and $\sigma_5(i) = -i$).

• $\sigma_6(\xi) = \xi'$, $\sigma_6(\xi') = -\xi$ (and so if σ_6 is indeed a $\mathbb{Q}$-homomorphism, $\sigma_6(\sqrt{2}) = -\sqrt{2}$, and $\sigma_6(i) = -i$).

• $\sigma_7(\xi) = -\xi'$, $\sigma_7(\xi') = \xi$ (and so if σ_7 is indeed a $\mathbb{Q}$-homomorphism, $\sigma_7(\sqrt{2}) = -\sqrt{2}$, and $\sigma_7(i) = -i$).

• $\sigma_8(\xi) = -\xi'$, $\sigma_8(\xi') = -\xi$ (and so if σ_8 is indeed a $\mathbb{Q}$-homomorphism, $\sigma_8(\sqrt{2}) = \sqrt{2}$, and $\sigma_8(i) = -i$).

We know $\sigma_1 \in G$. Also, since G is transitive on the roots of f and ξ is a root of f, we know: either σ_3 or σ_4 is in G; either σ_5 or σ_6 is in G; and either σ_7 or σ_8 is in G. Similarly, since ξ' is a root of f, we know: either σ_2 or σ_4 is in G; either σ_5 or σ_7 is in G; and either σ_6 or σ_8 is in G. Also, $\sigma_6^2 = \sigma_4 = \sigma_7^2$, $\sigma_6^3 = \sigma_7$, and $\sigma_7^3 = \sigma_6$. So if $|G| = 4$ then either $G = \{\sigma_1, \sigma_4, \sigma_6, \sigma_7\}$, or, in the case that $\sigma_6 \notin G$, $G = \{\sigma_1, \sigma_4, \sigma_5, \sigma_8\}$.

If $G = \{\sigma_1, \sigma_4, \sigma_6, \sigma_7\}$, then $i\sqrt{2} \in \phi(G)$, contradicting that, because $L : \mathbb{Q}$ is Galois, $\phi(G) = \mathbb{Q}$. If $G = \{\sigma_1, \sigma_4, \sigma_5, \sigma_8\}$ then $\sqrt{2} \in \phi(G)$, contradicting that, because $L : \mathbb{Q}$ is Galois, $\phi(G) = \mathbb{Q}$. Hence $|G| \neq 4$, and so we must have that $|G| = 8$. This implies that the maps $\sigma_1, \ldots, \sigma_8$ above are in fact $\mathbb{Q}$-homomorphisms, and $G = \{\sigma_1, \ldots, \sigma_8\}$. One easily checks that $\sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_8$ have order 2, and σ_6, σ_7 have order 4; also,

$$\sigma_3 = \sigma_6^2\sigma_2,\ \sigma_4 = \sigma_6^2,\ \sigma_5 = \sigma_6\sigma_2,\ \sigma_8 = \sigma_6^3\sigma_2.$$

Set $\sigma = \sigma_2$, $\tau = \sigma_6$. So $\langle\tau\rangle$ is an order 4 subgroup of G, with $\sigma \notin \langle\tau\rangle$. Hence $\langle\sigma, \tau\rangle = G$, since $\langle\sigma, \tau\rangle$ is a subgroup of G with at least 5 elements, and the order of a subgroup of G must divide $|G| = 8$. One easily checks that $\tau\sigma = \sigma\tau^3$, so

$$G = \langle\sigma, \tau : \ \sigma^2 = 1 = \tau^4, \ \tau\sigma = \sigma\tau^3 \ \rangle,$$

which is the dihedral group D_4.

Since $|G| = 8$, each proper, nontrivial subgroups of G has order 2 or 4. The subroups of order 2 are necessarily cyclic, and these are $\langle\sigma_j\rangle$ for $j = 2, 3, 4, 5, 8$. G has one cyclic subgroup of order 4, which is

$$\langle\sigma_6\rangle = \langle\sigma_7\rangle = \langle\tau\rangle = \{1, \tau, \tau^2, \tau^3\}.$$

The non-cyclic subgroups of G with order 4 cannot contain $\sigma_6 = \tau$ or $\sigma_7 = \tau^3$. Also, one easily checks that τ is in the subgroups

$$\langle\sigma, \tau\sigma\rangle, \ \langle\sigma, \tau^3\sigma\rangle, \ \langle\tau\sigma, \tau^2\sigma\rangle, \ \langle\tau^2\sigma, \tau^3\sigma\rangle,$$

so all of these subgroups must actually equal G. Hence the remaining non-cyclic subgroups of G with two generators are

$$\langle\sigma, \tau^2\rangle = \{1, \sigma, \tau^2, \tau^2\sigma\} = \langle\tau^2\sigma, \tau^2\rangle = \langle\sigma, \tau^2\sigma\rangle$$

and

$$\langle\tau\sigma, \tau^2\rangle = \{1, \tau\sigma, \tau^2, \tau^3\sigma\} = \langle\tau^3\sigma, \tau^2\rangle = \langle\tau\sigma, \tau^3\sigma\rangle.$$

From this, one sees that a subgroup of G with three (distinct) generators is either G or one of the subgroups we've already listed.

[**Note:** We could have argued that $|G| = 8$ by arguing that $f = t^4 - 2t^2 + 2$ is irreducible over $\mathbb{Q}(\sqrt{2})$, as follows. Since $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ and $\pm\xi, \pm\xi' \notin \mathbb{R}$, f does not have a linear factor in $\mathbb{Q}(\sqrt{2})[t]$. By the Quadratic Equation, $f = (t^2 - 1 + i)(t^2 - 1 - i)$, and as $i \notin \mathbb{Q}(\sqrt{2})$, these degree 2 factors of f do not lie in $\mathbb{Q}(\sqrt{2})[t]$. Hence $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[L : \mathbb{Q}(\sqrt{2})] = 4$.]

Now we determine the fixed subfields of L corresponding to the proper, nontrivial subgroups of G. We begin by determining the fixed fields of the subgroups of order 4.

We already noted that $\sqrt{2}, i, i\sqrt{2} \in L$. We see that $\tau(i\sqrt{2}) = i\sqrt{2}$, so $\mathbb{Q}(i\sqrt{2}) \subseteq \phi(\langle\tau\rangle)$. We know that $m_{i\sqrt{2}}(\mathbb{Q}) = t^2 + 2$ [since $i\sqrt{2}$ is a root of $t^2 + 2$ and $i\sqrt{2} \notin \mathbb{Q}$], so $[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = 2$. Hence by the Tower Law, $[L : \mathbb{Q}(i\sqrt{2})] = 4$. Since $\mathbb{Q}(i\sqrt{2}) \subseteq \phi(\langle\tau\rangle)$, we know that $[L : \phi(\langle\tau\rangle)] \leq 4$. Also, by the Fundamental Theorem of Galois Theory, we know that $\langle\tau\rangle = Gal(L : \phi(\langle\tau\rangle]$ and $|Gal(L : \phi(\langle\tau\rangle))| = [L : \phi(\langle\tau\rangle)]$. Hence $[L : \phi(\langle\tau\rangle)] = 4$, and thus $\phi(\langle\tau\rangle) = \mathbb{Q}(i\sqrt{2})$.

Now consider $\phi(\langle\sigma, \tau^2\rangle)$. We see that $\mathbb{Q}(i) \subseteq \phi(\langle\sigma, \tau^2\rangle)$. Since $m_i(\mathbb{Q}) = t^2 + 1$, we know that $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ and hence $[L : \mathbb{Q}(i)] = 4$. Consequently [arguing as in the preceding paragraph] $\mathbb{Q}(i) = \phi(\langle\sigma, \tau^2\rangle)$.

Somewhat similary, we see that $\mathbb{Q}(\sqrt{2}) \subseteq \phi(\langle\tau\sigma, \tau^2\rangle)$. Again, since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, we have $[L : \mathbb{Q}(\sqrt{2})] = 4$ and consequently $\mathbb{Q}(\sqrt{2}) = \phi(\langle\tau\sigma, \tau^2\rangle)$.

We have $\sigma(\xi) = \xi$, so $\mathbb{Q}(\xi) \subseteq \phi(\langle\sigma\rangle)$. Since $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$, we have $[L : \mathbb{Q}(\xi)] = 2 = |\langle\sigma\rangle|$, so $\phi(\langle\sigma\rangle) = \mathbb{Q}(\xi)$.

Similarly, $\phi(\langle\tau^2\sigma\rangle) = \mathbb{Q}(\xi')$.

Now, τ^2 fixes i and $\sqrt{2}$, and $[\mathbb{Q}(i,\sqrt{2}) : \mathbb{Q}] = 4$. [This is because $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $i \notin \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, and i is a root of t^2+1; hence $[\mathbb{Q}(\sqrt{2},i) : \mathbb{Q}(\sqrt{2})] = 2$.] Hence $\phi(\langle\tau^2\rangle) = \mathbb{Q}(\sqrt{2},i)$.

Now we consider the other two order 2 subgroups of G, which are $\langle\tau\sigma\rangle$ and $\langle\tau^3\sigma\rangle$; note that these are contained in $\langle\tau\sigma,\tau^2\rangle$, so their fixed fields contain $\mathbb{Q}(\sqrt{2}) = \phi(\langle\tau\sigma,\tau^2\rangle)$. First, let $E = \phi(\langle\tau\sigma\rangle)$. So $L = E(\xi)$, and $[L : E] = 2$ (since $|\langle\tau\sigma\rangle| = 2$). Thus $m_\xi(E)$ is a degree 2 polynomial that is fixed by $\tau\sigma$, that divides f and, in $L[t]$, is divisible by $t-\xi$. So $m_\xi(E)$ is one of the following polynomials:

$$f_1 = (t-\xi)(t+\xi) = t^2 - \xi^2 = t^2 - (1+i),$$
$$f_2 = (t-\xi)(t-\xi') = t^2 - (\xi+\xi')t + \sqrt{2},$$
$$f_3 = (t-\xi)(t+\xi') = t^2 - (\xi-\xi')t - \sqrt{2}.$$

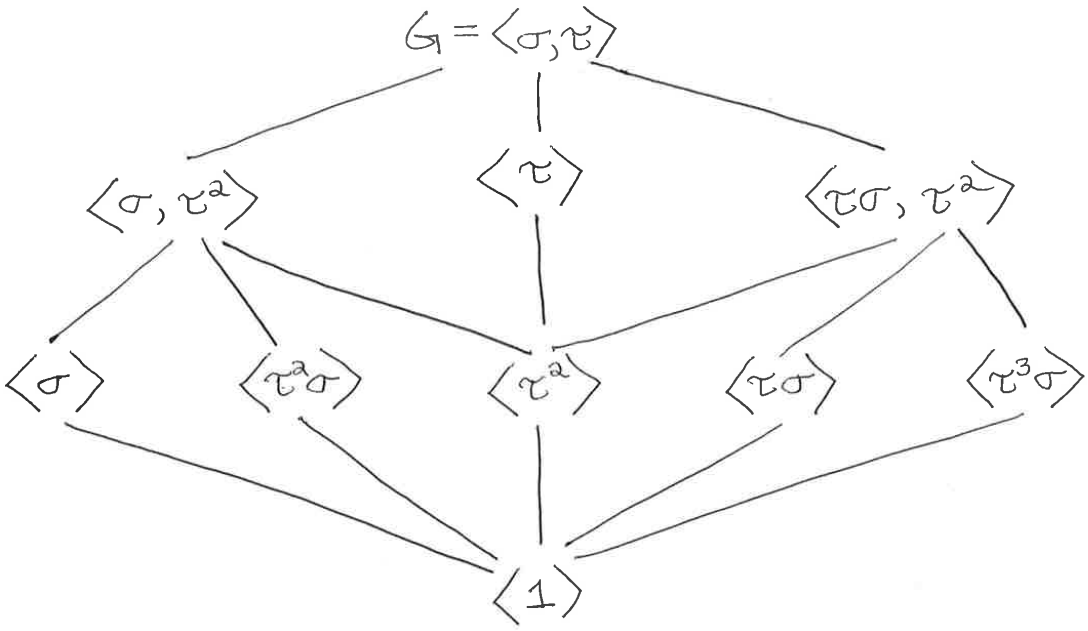
We know that $\tau\sigma$ fixes $\sqrt{2}$. Checking, we see that $\tau\sigma$ fixes $\xi+\xi'$, so we must have $m_\xi(E) = f_2$ [recall that $m_\xi(E)$ is unique]. Also note that $(\xi+\xi')^2 = 2+2\sqrt{2}$, so $\sqrt{2} \in \mathbb{Q}(\xi+\xi')$ and hence $f_2 \in \mathbb{Q}(\xi+\xi')[t]$. Thus $m_\xi(\mathbb{Q}(\xi+\xi'))$ divides f_2, which means that $[L : \mathbb{Q}(\xi+\xi')] \leq \deg f_2 = 2$. Hence we have

$$2[E : \mathbb{Q}(\xi+\xi')] = [L : E][E : \mathbb{Q}(\xi+\xi')] = [L : \mathbb{Q}(\xi+\xi')] \leq 2.$$

Hence $[E : \mathbb{Q}(\xi+\xi')] = 1$, meaning $\mathbb{Q}(\xi+\xi') = E = \phi(\langle\tau\sigma\rangle)$.

Noting that $\tau^3\sigma$ fixes $\xi-\xi'$, a virtually identical argument shows that $\mathbb{Q}(\xi-\xi') = \phi(\langle\tau^3\sigma\rangle)$.

(See next page for a diagram of the subgroups of G and the corresponding fixed fields of $L = \mathbb{Q}(\xi,\xi')$.)



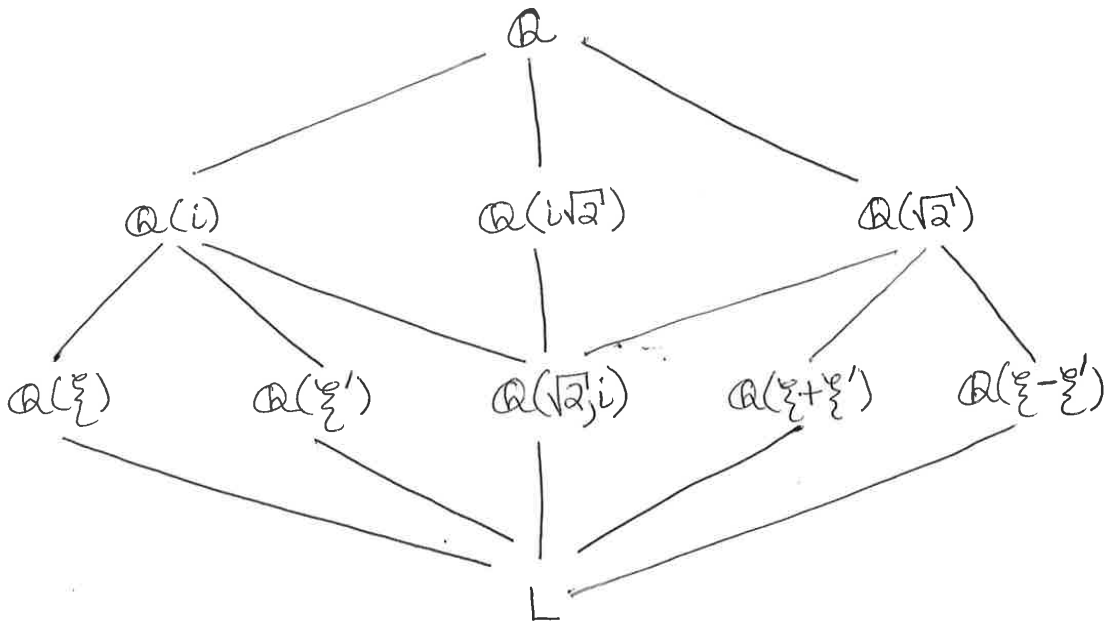


Diagram of the subgroups of $G = Gal(L:\mathbb{Q})$ and the corresponding fixed fields where $L:\mathbb{Q}$ is a splitting field extension for $f = t^4 - 2t^2 + 2$ and $\xi = \sqrt{1+i}$, $\xi' = \sqrt{1-i}$.

Theorem 11.2. *Let $E : K$ and $F : K$ be finite extensions with L a field containing both E and F [so for instance, we could take $L = \overline{K}$].*

(a) *When $E : K$ is Galois, then $EF : F$ is Galois and $Gal(EF : F) \simeq Gal(E : E \cap F)$.*
(b) *When $E : K$ and $F : K$ are both Galois, then $EF : K$ and $E \cap F : K$ are both Galois, and*

$$Gal(EF : E \cap F) \simeq Gal(E : E \cap F) \times Gal(F : E \cap F).$$

Proof. (a) Suppose $E : K$ is Galois. By Theorems 6.8 and 7.8, the extension $EF : F$ is Galois. Take $\sigma \in Gal(EF : F)$. Then $\sigma|_E$ gives us a K-homomorphism from E into EF. For $\alpha \in E$, we know that $\sigma(\alpha)$ is a root of $m_\alpha(K)$, and since $E : K$ is Galois, we have $\sigma(\alpha) \in E$. Thus $\sigma(E) \subseteq E$. So by Theorem 3.4, $\sigma|_E$ is an automorphism of E. Further, for $\alpha \in E \cap F$, we know that $\sigma(\alpha) = \alpha$ since σ is an F-homomorphism. Therefore the map $\psi : Gal(EF : F) \to Gal(E : E \cap F)$ given by $\sigma \mapsto \sigma|_E$ is a homomorphism. Also, $\sigma \in \ker \psi$ if and only if $\sigma|_E = id_E$. We know $\sigma|_F = id_F$, so $\sigma|_E = id_E$ if and only if $\sigma = \sigma|_{EF} = id_{EF}$. Hence $\ker \psi = \{id_{EF}\}$, meaning ψ is injective. To show ψ is surjective, let $H = \psi(Gal(EF : F))$, which is a subgroup of $Gal(E : E \cap F)$. Using Theorem 11.1, we have

$$\begin{aligned} Fix_E(H) &= \{\alpha \in E : \ \sigma|_E(\alpha) = \sigma(\alpha) = \alpha \ \forall \sigma \in Gal(EF : F) \ \} \\ &= \{\alpha \in E : \ \alpha \in Fix_{EF}(Gal(EF : F)) = F \ \} \\ &= E \cap F. \end{aligned}$$

Hence by Theorem 11.1,

$$\psi(Gal(EF : F)) = H = Gal(I : Fix_E(H)) = Gal(E : E \cap F),$$

meaning ψ is surjective. Therefore by the 1st Isomorphism Theorem of Group Theory, $Gal(EF : F) \simeq Gal(E : E \cap F)$.

(b) Suppose $E : K$ and $F : K$ are both Galois. By Thorems 6.8 and 7.8, the extensions $EF : K$ and $E \cap F : K$ are also Galois. As an exercise, one shows that $\sigma \mapsto (\sigma|_E, \sigma|_F)$ gives us a homomorphism $\omega : Gal(EF : E \cap F) \to Gal(E : E \cap F) \times Gal(F : E \cap F)$. We have that $\ker \omega$ is trivial, since if $\sigma \in Gal(EF : E \cap F)$ fixes E and F pointwise then σ fixes EF pointwise. Also, $Gal(EF : F) \subseteq Gal(EF : E \cap F)$, so by (a),

$$\omega(Gal(EF : F)) = Gal(E : E \cap F) \times \{id_F\}.$$

Similarly, $\omega(Gal(EF : E)) = \{id_E\} \times Gal(E : E \cap E)$. Hence as the image of ω is a subgroup of $Gal(EF : K)$, we have

$$Gal(E : E \cap F) \times Gal(F : E \cap F) = \omega(Gal(EF : E \cap F)).$$

Thus ω is bijective, proving (b). □

Remark. Suppose $L : K$ is a finite Galois extension. For all $\alpha \in L$, by Corollary 6.6, G acts transitively on the roots of $m_\alpha(K)$.

12. Finite fields

Throughout this section, let K be a finite field. Recall that this means $\mathrm{char}K = p$ where p is a prime, and $|K| = p^m$ for some $m \in \mathbb{Z}_+$. Also, K contains a subfield isomorphic to $\mathbb{Z}/p\mathbb{Z}$, called the prime subfield of K, which is generated as an additive subgroup of K by the element $1 = 1_K$. Thus K is a field extension of its prime subfield, with degree m. We also know that as a multiplicative group, $K^\times$ is cyclic.

Theorem 12.1. *Let p be a prime, and let $q = p^n$ be a positive power of p. Then:*

(a) *There exists a field of order q, and this field is unique up to isomorphism (and is denoted by $\mathbb{F}_q$).*
(b) *All elements of $\mathbb{F}_q$ satisfy the equation $t^q = t$, and hence $\mathbb{F}_q : \mathbb{F}_p$ is a splitting field extension for $t^q - t$.*
(c) *There is a unique copy of $\mathbb{F}_q$ inside any alebraically closed field containing $\mathbb{F}_p$.*

Proof. Put $K = \mathbb{F}_p$, and let $L : K$ be a splitting field extension for $f = t^q - t$. By Corollary 8.6, f is separable over K and hence f has q distinct roots in L. Write R for the set of roots of f in L. Let $\phi : L \to L$ be the Frobenius map (so $\phi(\alpha) = \alpha^p$). [Recall that by Corollary 8.5, $\phi \in Aut(L)$.] Then $\phi^n(\alpha) = \alpha^{p^n}$ for any $\alpha \in L$. So the set of elements of L fixed by ϕ^n are exactly the roots of f, or in other words,

$$R = \{\alpha \in L : \ \phi^n(\alpha) = \alpha \ \}.$$

Note that $|R| = q$. So R is the subset of L that is fixed by the group $\langle \phi^n \rangle$, which is a subgroup of $Gal(L : K)$ [recall that by Fermat's Little Theorem, every element of $K \simeq \mathbb{Z}/p\mathbb{Z}$ is fixed by the map $\alpha \mapsto \alpha^p$ and thus $\alpha \in K$ is fixed by the map $\alpha \mapsto \alpha^{p^n}$]. Hence R is a subfield of L, and every element of R is a root of f. Thus $R : K$ is a splitting field for f with $R \subseteq L$, so we must have $R = L$. Hence L is a field with q elements.

Now suppose that $M : K$ is a field extension with $|M| = q$. We know that $M^\times$ is a group with $q - 1$ elements, so every element of $M^\times$ is a root of $t^{q-1} - 1$, and so M is a root of $t^q - t$. We also know that $M : K$ is a field extension [since the prime subfield of M is isomorphic to $\mathbb{F}_p$], so $M : K$ is a splitting field extension for f. By Theorem 5.4, $M \simeq L$.

Thus we have proved (a) and (b).

To prove (c), note that any algebraically closed field containing $\mathbb{F}_p$ has a unique subfield E that is a splitting field for $t^q - t$, and hence $E \simeq \mathbb{F}_q$. □

As an exercise, one proves the following.

Theorem 12.2. *Let p be a prime and $q = p^n$ where $n \in \mathbb{Z}_+$. Then:*

(a) *The field extension $\mathbb{F}_q : \mathbb{F}_p$ is Galois with $Gal(\mathbb{F}_q : \mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$.*
(b) *$\mathbb{F}_q$ contains a subfield of order p^d if and only if $d|n$. If $d|n$, then there is a unique subfield of $\mathbb{F}_q$ of order p^d.*

13. Solvability by radicals: quadratic, cubic, and quartic polynomials

We are familiar with the fact that when K is a field with characteristic different from 2, then quadratic equations can be solved by adjoining square-roots: Say $f = at^2+bt+c \in K[t]$. Then $f = (2at+b)^2-(b^2-4ac)$ is solvable in $K(\sqrt{b^2-4ac})$ with roots $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$. With α_1 a root of f and $L = K(\alpha_1)$, we have $f = a(t-\alpha_1)(t-\alpha_2)$ where α_2 is necessarily an element of L. Hence $L : K$ is a splitting field extension for f. We have $Gal(L : K) = \{id_L\}$ if $\alpha_1 \in K$ or if $\alpha_1 = \alpha_2$; so $Gal(L : K) = \{id_L\}$ if $b^2 - 4ac$ is a square in K. In the case that $b^2 - 4ac$ is not a square in K, then $Gal(L : K) = \{id_L, \tau\}$ where $\tau(\alpha_1) = \alpha_2$ (note that $\alpha_2 = -b/a - \alpha_1$).

Definitions. Suppose that $L : K$ is a field extension, and $\beta \in L$. We say that β is radical over K when $\beta^n \in K$ for some $n \in \mathbb{Z}_+$ (so $\beta = \alpha^{1/n}$ for some $\alpha \in K$ and some $n \in \mathbb{Z}_+$). We say that $L : K$ is an extension by radicals when there is a tower of field extensions $L = L_r : L_{r-1} : \cdots : L_0 = K$ such that $L_i = L_{i-1}(\beta_i)$ with β_i radical over L_{i-1} $(1 \le i \le r)$. We say $f \in K[t]$ is solvable by radicals if there is a radical extension of K over which f splits.

We want to explore when a polynomial over a field K is solvable by radicals. First, the "quick and dirty" approach.

Cubic polynomials (approach of Fontano and of Cardano, circa 1535). Since we work over a field K, it suffices to consider monic polynomials. Suppose $\mathrm{char}K \neq 2, 3$ and $f = t^3 + a_2t^2 + a_1t + a_0 \in K[t]$.

Complete the cube:

$$\begin{aligned} 27f &= (3t + a_2)^3 + 3(3a_1 - a_2^2)(3t + a_2) + (27a_0 + 2a_2^3 - 9a_1a_2) \\ &= y^3 + 3b_1y + b_0 \end{aligned}$$

where $y = 3t + a_2$, $b_1 = 3a_1 - a_2^2$, $b_0 = 27a_0 + 2a_2^3 - 9a_1a_2$. Thus $f \in K[t]$ is solvable by radicals if and only if $y^3+b_1y+b_0 \in K[y]$ is solvable by radicals. [Note that $27 \in K$ with $27 \neq 0$ since $\mathrm{char}K \neq 3$, and that f splits over a field L if and only if $y^3 + 3b_1y + b_0$ splits over L.]

Auxiliary equation: Suppose we can find $u, v \in \overline{K}$ so that $u \neq 0$, $uv = -b_1$ and $u^3 + v^3 = -b_0$; then

$$\begin{aligned} (u + v)^3 + 3b_1(u + v) + b_0 &= (u^3 + v^3) + 3uv(u + v) + 3b_1(u + v) + b_0 \\ &= 0. \end{aligned}$$

So with $y = u + v$, we find a solution to $y^3 + 3b_1y + b_0$. Hence we proceed as follows: Assume $u \neq 0$ and put $v = -b_1/u$. Then

$$\begin{aligned} &(u + v)^3 + 3b_1(u + v) + b_0 = 0 \\ &\iff (u - b_1/u)^3 + 3b_1(u + b_1/u) + b_0 = 0 \\ &\iff u^3 - b_1^3/u^3 - 3ub_1/u + 3b_1^2/u + 3b_1u - 3b_1^2/u + b_0 = 0 \\ &\iff u^3 - b_1^3/u^3 + b_0 = 0 \\ &\iff (u^3)^2 + b_1u^3 - b_1^3 = 0. \end{aligned}$$

This has the solution

$$u^3 = \frac{-b_0 \pm \sqrt{b_0^2 + 4b_1^3}}{2}$$

and then $v^3 = -b_0 - u^3$. Thus both u and v are given by taking cube roots of elements of $K_1 = K(\sqrt{b_0^2 + 4b_1^3})$ (which is a radical extension of K), and hence u, v are elements of a radical extension K_2 of K. Then with these choices for u, v, one root of f is

$$u + v = \sqrt[3]{\frac{-b_0 + \sqrt{b_0^2 + 4b_1^3}}{2}} + \sqrt[3]{\frac{-b_0 - \sqrt{b_0^2 + 4b_1^3}}{2}}.$$

Thus over K_2, $y^3 + b_1 y + b_0 = (t - u - v)(t^2 + c_1 t + c_0)$ for some $c_1, c_0 \in K_2$. Using the quadratic equation, we can find a radical extension L of K_2 over which $t^2 + c_1 t + c_0$ splits.

The above discussion presumes that $u \neq 0$, where $u^3 = \frac{-b_0 \pm \sqrt{b_0^2 + 4b_1^3}}{2}$. We have

$$\begin{aligned} -b_0 \pm \sqrt{b_0^2 + 4b_1^3} = 0 &\iff b_0 = 0 = b_0^2 + 4b_1^3 \\ &\iff b_0 = 0 = b_1 \\ &\iff f = y^3 = (t - a_2/3)^3. \end{aligned}$$

So in any case, $f = t^3 + a_2 t^2 + a_1 t + a_0 \in K[t]$ splits over a rational extension of K when $\mathrm{char} K \neq 2, 3$.

Quartic polynomials (approach of Cardano, circa 1545). Suppose $\mathrm{char} K \neq 2, 3$ and $f = t^4 + a_3 t^3 + a_2 t^2 + a_1 t + a_0 \in K[t]$.

Complete the 4th power:

$$64 f = y^4 + b_2 y^2 + b_1 y + b_0$$

where $y = 4t + a_3$, and $b_2, b_1, b_0 \in K$ are given by polynomials in the a_i. So $f \in K[t]$ is solvable by radicals if and only if $g = y^4 + b_2 y^2 + b_1 y + b_0 \in K[y]$ is solvable by radicals; also, a splitting field for f is a splitting field for g.

Auxiliary equation: We want to find r in a radical extension of K so that

$$g = y^4 + b_2 y^2 + b_1 y + b_0 = (y^2 - r)^2 + (b_2 - 2r)(y - \beta)^2$$

for some β in a radical extension of K, as then we can find a root of g in a radical extension of K. Note that we have $g = (y^2 + r)^2$ for some $r \in \overline{K}$ if and only if $b_1 = 0$, $b_0 = b_2^2/4$, and $r = b_2/2$ (which is an element of K). Thus when $g = (y^2 + r)^2$ for some $r \in \overline{K}$, we have that g splits over K and $r = b_2/2$.

Suppose $r \in \overline{K}$ with $r \neq b_2/2$. Then in $\overline{K}[y]$,

$$\begin{aligned} g - (y^2 + r)^2 = (b_2 - 2r) &\left(y + \frac{b_1 + \sqrt{b_1^2 - 4(b_2 - 2r)(b_0 - r^2)}}{2(b_2 - 2r)} \right) \\ &\cdot \left(y + \frac{b_1 - \sqrt{b_1^2 - 4(b_2 - 2r)(b_0 - r^2)}}{2(b_2 - 2r)} \right). \end{aligned}$$

Hence we have $g = (y^2+r)^2 + (b_2-2r)(y-\beta)^2$ for some $\beta \in \overline{K}$ if and only if

$$b_1^2 = 4(b_2-2r)(b_0-r^2), \text{ and } \beta = \frac{b_1}{2(b_2-2r)}.$$

We can find r in a radical extension L of K so that $b_1^2 - 4(b_2-2r)(b_0-r^2) = 0$, and hence $\beta = \frac{b_1}{2(b_2-2r)} \in L$. With these choices of r and β, we can find a root of

$$y^2 + r - \sqrt{b_2-2r}(y-\beta)$$

in a radical extension M of L. Hence M is a radical extension of K containing a root α of g. So $g = (y-\alpha)h$ where h is a cubic polynomial in $M[y]$, and by our previous discussion about cubic polynomials, we can find a radical extension of M over which h splits. Hence there is a radical extension of K over which f splits.

Galois groups for splitting fields of cubic and quartic polynomials. Now we explore solvability of cubic and quartic polynomials in a less ad hoc fashion, so that we also compute the Galois groups of the splitting field extensions for these polynomials. We first introduce the discriminant of a polynomial, which detects whether multiple roots of a polynomial.

Take $f \in K[t]$, $\deg f \geq 1$. In $\overline{K}[t]$, $f = a\prod_{i=1}^n (t-\alpha_i)$ (so $a \in K$). Set

$$D = D(f) = a^{2n-2} \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j)^2.$$

We call $D(f)$ the discriminant of f. So $D(f) = 0$ if and only if f has a multiple root; hence if $D(f) \neq 0$ then f is separable over K.

Note that $D(f)$ is independent of the ordering of the roots $\alpha_1, \ldots, \alpha_n$, so for $\varphi \in S_n$, the symmetric group on $\{1, 2, \ldots, n\}$, we have

$$D = D(f) = a^{2n-2} \prod_{1\leq i<j\leq n} (\alpha_{\varphi(i)} - \alpha_{\varphi(j)})^2.$$

Let $L = K(\alpha_1, \ldots, \alpha_n)$, and take

$$d = d(f) = a^{n-1} \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j),$$

a square root of $D(f)$. Note that as $L : K$ is a splitting field extension for f, $L : K$ is normal. We know from Proposition 3.1 that $Gal(L : K)$ is isomorphic to some subgroup H of S_n. For $\varphi \in H$, φ corresponds to $\sigma_\varphi \in Gal(L : K)$ determined by $\sigma_\varphi(\alpha_i) = \alpha_{\varphi(i)}$. If φ is a transposition, then $\varphi = (k\ m)$ for some k, m with $1 \leq k < m \leq n$, and hence

$$\sigma_\varphi\left(\prod_{i<j}(\alpha_i - \alpha_j)\right) = (\alpha_m - \alpha_k) \prod_{\substack{i<j \\ i,j\neq k,m}} (\alpha_i - \alpha_j) = -\prod_{i<j}(\alpha_i - \alpha_j).$$

Consequently when φ is a product of ℓ transpositions, then we get $\sigma_\varphi(d) = (-1)^\ell d$; so $\sigma_\varphi(d) = d$ if φ is an even permutations, and $\sigma_\varphi = -d$ if φ is an odd permutation. Note that $\sigma_\varphi(D) = D$ for all $\varphi \in H$, so if $L : K$ is Galois then $D \in K = Fix_L(Gal(L : K))$.

The Galois group of a separable cubic polynomial. Suppose $f \in K[t]$ is separable and irreiducible over K with $\deg f = 3$. Thus with $f = a(t - \alpha_1)(t - \alpha_2)(t - \alpha_3)$, $\alpha_1, \alpha_2, \alpha_3 \in \overline{K}$, we know that

$$d = d(f) = a^2 \prod_{i<j} (\alpha_i - \alpha_j) \neq 0.$$

Let $L = K(\alpha_1, \alpha_2, \alpha_3)$. As discussed above, $Gal(L : K) \simeq H$ for some subgroup H of S_3. Hence $|Gal(L : K)|$ divides 6. Also, by Theorem 3.2, $Gal(L : K)$ is transitive on the roots of f (which are distinct), so $|Gal(L : K)| \geq 3$. Hence $|Gal(L : K)| = 3$ or 6. As A_3 is the only subgroup of S_3 with order 3, we have $Gal(L : K) \simeq A_3$ or S_3. Hence $\sigma(d) = d$ for all $\sigma \in Gal(L : K)$ if and only if $Gal(L : K) \simeq A_3$. This proves the following.

Theorem 13.1. *Suppose that $f \in K[t]$ is a separable and irreducible over K with $\deg f = 3$. Let $L : K$ be a splitting field extension for f. Then $Gal(L : K) \simeq A_3$ if $D(f)$ has a square root in K; otherwise, $Gal(L : K) \simeq S_3$.*

The Galois group of a separable quartic polynomial. Suppose $\mathrm{char}K \neq 2$, and $f = t^4 + a_3t^3 + a_2t^2 + a_1t + a_0 \in K[t]$. So by Theorem 8.2, f is separable over K. Then as above, making the change of variables $y = 4t + a_3$, we have

$$64f = g = y^4 + b_2y^2 + b_1y + b_0 \in K[y].$$

Let $\alpha_1, \ldots, \alpha_4 \in \overline{K}$ denote the roots of g, and set $L = K(\alpha_1, \ldots, \alpha_4)$. So the roots of f are $\beta_i = \alpha_i + \frac{a_3}{4a_4}$, and hence $L : K$ is a splitting field for g and for f. By Corollary 7.6, $L : K$ is separable and hence (also by Corollary 7.6) g is also separable over K. (Hence $D(g) \neq 0$.)

Note that as the coefficient of y^3 in g is 0, we have $\alpha_4 = -\alpha_1 - \alpha_2 - \alpha_3$.

The resolvant polynomial of g is defined to be

$$r = r(g) = (y - u)(y - v)(y - w)$$

where

$$\begin{aligned} u &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = -(\alpha_1 + \alpha_2)^2, \\ v &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) = -(\alpha_1 + \alpha_3)^2, \\ w &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) = -(\alpha_1 + \alpha_4)^2 = -(\alpha_2 + \alpha_3)^2. \end{aligned}$$

One can check that

$$r = y^3 - 2b_2y^2 + (b_2^2 - rb_0)y + b_1^2 \in K[y],$$

and so with $F = K(u, v, w)$, $F : K$ is a splitting field extension for r. Since $u - v = (\alpha_1 - \alpha_4)(\alpha_3 - \alpha_2)$, $u - w = (\alpha_1 - \alpha_3)(\alpha_4 - \alpha_2)$, $v - w = (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_2)$, we find that $D(r) = D(g)$. Thus $D(r) \neq 0$, which means that r is separable over K.

To solve for the roots of g, we first solve for the roots of r (we can use Cardano's method if $\mathrm{char}K \neq 3$). Then

$$\begin{aligned} u' &= \alpha_1 + \alpha_2 \text{ (a square root of } -u), \\ v' &= \alpha_1 + \alpha_3 \text{ (a square root of } -v), \\ w' &= \alpha_1 + \alpha_4 \text{ (a square root of } -w). \end{aligned}$$

Thus

$$u'v'w' = \alpha_1^2 \sum_i \alpha_i + \sum_{i<j<k} \alpha_i\alpha_j\alpha_k = -b_1$$

since $\sum_i \alpha_i = 0$. Hence we have

$$\alpha_1 = \frac{1}{2}(u' + v' + w'),\ \alpha_2 = \frac{1}{2}(u' - v' - w'),$$
$$\alpha_3 = \frac{1}{2}(-u' + v' - w'),\ \alpha_4 = \frac{1}{2}(-u' - v' + w').$$

As $u'v'w' = -b_1 \in K$, we have $F = K(u, v, w) = K(u, v)$ and $K(u', v', w') = K(u', v')$. Also note that $[K(\sqrt{u}, v) : K(u, v)] \leq 2$, $[K(\sqrt{u}, \sqrt{v}) : K(\sqrt{u}, v)] \leq 2$, so

$$[K(u', v') : F] = [K(v', v') : K(u, v)] \leq r.$$

We also have $\alpha_1, \ldots, \alpha_4 \in K(u', v')$, so

$$[L : F] \leq [K(u', v') : F] \leq 4.$$

We know that $Gal(F : K)$ is isomorphic to a subgroup of S_3 (snce $F : K$ is a splitting field extension for a polynomial of degree 3), and similarly, $Gal(L : K)$ is isomorphic to a subgroup of S_4.

A more detailed exploration (as in §7.6 of Grillet's book *Algebra*) gives us the following (recall that $L : K$ is a splitting field extension for f and for g).

Theorem 13.2. *Suppose that charK $\neq 2$, and that $f \in K[t]$ is separable and irreducible over K with* $\deg f = 4$. *Let g and r be the polynomials as defined above, and let $F : K$ be a splitting field extension for r. Then we have the following.*

(a) $[F : K]$ *divides 6.*
(b) *If* $[F : K] = 6$ *then* $Gal(L : K) \simeq S_4$.
(c) *If* $[F : K] = 3$ *then* $Gal(L : K) \simeq A_4$.
(d) *If* $[F : K] = 2$ *then* $Gal(L : K) \simeq D_4$ *if f is irreiducible over F, otherwise* $Gal(L : K) \simeq \mathbb{Z}/4\mathbb{Z}$.
(e) *If* $[F : K] = 1$ *then* $Gal(L : K) \simeq V_4$.

(Recall that

$$D_4 = \langle a, b :\ a^4 = b^2 = 1,\ ba = a^3b \rangle,$$

the dihedral group of order 8, and

$$V_4 = \langle a, b, c :\ a^2 = b^2 = c^2 = 1,\ ab = c \rangle,$$

the Klein-4 group.)

14. Higher degree polynomials and Hilbert's 13th Problem

We look at a general method of simplifying equations using a unified approach of Tschirnhaus (circa 1680).

Suppose for simplicity that char$K = 0$. Let

$$f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in K[t]$$

by irreducible over K. Let $L : K$ be a splitting field extension for f; so $L : K$ is a Galois extension (recall that f is separable over K since char$K = 0$). Let $\theta_1, \ldots, \theta_n$ be the roots of f in L. Put

$$\phi_i = y_0 + y_1\theta_i + \cdots + y_{n-1}\theta_i^{n-1} \ (1 \leq i \leq n),$$

where the y_i are indeterminates (so for each i, $\phi_i \in L[y_0, \ldots, y_{n-1}]$). Now consider the polynomial

$$\begin{aligned} g(x) &= (x - \phi_1)(x - \phi_2)\cdots(x - \phi_n) \\ &= x^n + b_1x^{n-1} + \cdots + b_n \in L[y_0, \ldots, y_{n-1}][x]. \end{aligned}$$

(The coefficients of g are known as elementary symmetric polynomials in $\phi_1, \ldots, \phi_n$.) So

$$b_1 = -(\phi_1 + \cdots + \phi_n) = -(ny_0 + y_1 \sum \theta_i + y_2 \sum \theta_i^2 + \cdots + y_{n-1}\theta_i^{n-1},$$

$$b_2 = \sum_{i \neq j} \phi_i\phi_j,$$

and so on. Each element of $Gal(L : K)$ extends naturally to an isomorphism of $L[y_0, \ldots, y_{n-1}]$ that fixes each y_i. As each $\sigma \in Gal(L : K)$ permutes $\theta_1, \ldots, \theta_n$, each $\sigma \in Gal(L : K)$ permutes $\phi_1, \ldots, \phi_n$. Hence (extending $\sigma \in Gal(L : K)$ to an isomorphism on $L[y_0, \ldots, y_{n-1}][x]$ by setting $\sigma(x) = x$), we see that g is fixed by $Gal(L : K)$. Hence for each i, $b_i \in K[y_0, \ldots, y_{n-1}]$.

The strategy now is to try to choose $y_0, \ldots, y_{n-1}$ in a radical extension of K in such a way that the polynomial g simplifies so as to be solvable in a simpler field.

Example 0. When $n = 2$, the polynomial $b_1(y_0, y_1)$ is linear in the variables y_0, y_1 over $K[y_0, y_1]$, so we can find $\gamma_0, \gamma_1 \in K^\times$ so that $b_1(\gamma_0, \gamma_1) = 0$ (recall that $\theta_1 + \theta_2 = -a_1 \in K$). Then taking $y_0 = \gamma_0$, $y_1 = \gamma_1$, we have $b_2 \in K$,

$$g(x) = x^2 + b_2 \in K[x],$$

and $g(x) = 0$ can be solved by radicals, with [specific] roots $\widehat{\phi}_1, \widehat{\phi}_2 \in M$ where $M : K$ is a radical extension. Now we solve

$$\widehat{\phi}_i = \gamma_0 + \gamma_1\theta_i$$

for θ_i $(i = 1, 2)$.

Example 1. When $n \geq 3$, we can solve the equations

$$b_1(y_0, y_1, \ldots, y_{n-1}) = 0 \text{ (linear)}$$

$$b_2(y_0, y_1, \ldots, y_{n-1}) = 0 \text{ (quadratic)}$$

by substituting for y_0 from the linear equation into the quadratic equation. we are then left with a quadratic equation in in $y_1, \ldots, y_{n-1}$, and by fixing $y_3, \ldots, y_{n-1}$ to be 0, we are left with a (homogeneous) quadratic in 2 variables to solve. This can be solved by radicals (take $y_2 = 1$ and solve for y_1). Say $y_i = \gamma_i$ is a solution. Then on substituting, we find that

$$g(x) = x^n + b_3x^{n-3} + \cdots + b_n.$$

When $n = 3$, this gives $g(x) = x^3 + b_3$, and we can solve $g(x) = 0$ by radicals to obtain solutions $\widehat{\phi}_1, \widehat{\phi}_2, \widehat{\phi}_3$. Now solve for θ_i from

$$\widehat{\phi}_i = \gamma_0 + \gamma_1\theta_i + \gamma_2\theta_i^2 \ (i = 1, 2, 3).$$

Again, we can do this by radicals.

Example 2. When $n \geq 4$, we can solve

$$b_1(y_0, y_1, \ldots, y_{n-1}) = 0 \text{ (linear)}$$
$$b_3(y_0, y_1, \ldots, y_{n-1}) = 0 \text{ (cubic)}$$

by substituting for y_0 from the linear equation into the cubic equation. Put $y_3, \ldots, y_{n-1} = 0$ and $y_2 = 1$, and solve the cubic. Say this gives us $y_i = \gamma_i$. Then on substituting, we find that

$$g(x) = x^n + b_2 x^{n-2} + b_4 x^{n-4} + \sum_{j=5}^{n} b_j x^{n-j}.$$

When $n = 4$, this gives $x^4 + b_2 x^2 + b_4$, which can be solved by radicals for x^2, and hence for x, with solutions $\widehat{\phi}_1, \ldots, \widehat{\phi}_4$. Now solve for θ_i from

$$\widehat{\phi}_i = \gamma_0 + \gamma_1 \theta_i + \gamma_2 \theta_i^2 + \gamma_3 \theta^3 \ (i = 1, 2, 3, 4).$$

Again, we can do this by radical extensions, and hence θ_i is obtained through a tower of radical extensions.

Example 3. When $n \geq 5$, we can solve

$$b_1(y_0, y_1, \ldots, y_{n-1}) = 0 \text{ (linear)}$$
$$b_2(y_0, y_1, \ldots, y_{n-1}) = 0 \text{ (quadratic)}$$
$$b_3(y_0, y_1, \ldots, y_{n-1}) = 0 \text{ (cubic)}$$

in a tower of radical extensions.

Idea: First substitute for y_0 from the linear equation, then diagonalise the quadratic so that b_2 takes the shape

$$\lambda_1 z_1^2 + \cdots + \lambda_{n-1} z_{n-1}^2 = 0$$

with z_i K-linear in $y_1, \ldots, y_{n-1}$, and $\lambda_1, \ldots, \lambda_{n-1} \in K$. With this linear change of variables, $b_3(y_0, \ldots, y_{n-1}) = 0$ takes the shape $b_3'(z_1, \ldots, z_{n-1}) = 0$ with b_3' cubic over K.

Now put $z_5, \ldots, z_{n-1} = 0$, solve $\lambda_1 z_1^2 + \lambda_2 z_2^2 = 0$ and $\lambda_3 z_3^2 + \lambda_4 z_4^2 = 0$ with $z_2 = z_4 = 1$. Say $\underline{z} = \underline{\gamma}$, and substitute $\underline{z} = (\omega\gamma_1, \omega\gamma_2, \gamma_3, \gamma_4, \ldots, \gamma_{n-1})$ into the cubic equation. Then $b_3'(z_1, \ldots, z_{n-1}) = B_3(\omega)$ with B_3 a cubic polynomial in ω with coefficients from a tower of quadratic extensions. The equation $B_3(\omega)$ can be solved by radicals over its field of coefficients, and hence over K. Back-substituting such a solution ω, we obtain

$$g(x) = x^n + b_4 x^{n-4} + \cdots + b_n.$$

When $n = 5$, this equation takes the shape $x^5 + ax + b = 0$, i.e.

$$(x/\sqrt[5]{b})^5 + a\ {}^{-4/5}\sqrt{b}(x/\sqrt[5]{b}) + 1 = 0.$$

Then it suffices to solve the equation

$$y^5 + ay + 1 = 0.$$

This cannot always be done in a radical extension, but we have shown that quintics can be solved in towers of radical extensions if we also adjoin roots of a 1-parameter set of polynomials $Y65 + ay + 1$ (where a is the parameter).

Hilbert's 13th Problem: How many parameters $k(n)$ are required if we are to solve polynomials of degree n by towers of radical extensions and the addition of roots of polynomials of a $k(n)$-parameter family of polynomials?

degree n	# of additional parameters required	known results
2	0	solvable by radicals
3	0	solvable by radicals
4	0	solvable by radicals
5	1	
6	2	
7	3	
8	4	
9	4	Hilbert, 1909
10	5	
11	6	
$\vdots$	$\vdots$	
n	$n-5$	
$\vdots$	$\vdots$	
157	151	Segre, 1944
$\vdots$	$\vdots$	
n	$n-6$	
$\vdots$	$\vdots$	
n	$n-k(n)$	$k(n) \to \infty$ as $n \to \infty$ (Brauer, 1945) $k(n) \geq \log_2 \log_2(n)$ (Wooley, 1996)

15. Cyclotomic polynomials and cyclotomic extensions

Definition. For $n \in \mathbb{Z}_+$, we say $\varepsilon \in K$ is an nth root of unity if $\varepsilon^n = 1$. We say $\varepsilon \in K$ is a primitive nth root of unity if $\varepsilon^n = 1$ and for $k \in \mathbb{Z}_+$ with $k < n$, $\varepsilon^k \neq 1$. (Thus $\varepsilon \in K$ is a primitive nth root of unity if ε has order n in the multiplicative group $K^\times$.)

Definition. For $n \in \mathbb{Z}_+$, the nth cyclotomic polynomial is

$$\Phi_n = \prod_{\varepsilon} (t - \varepsilon) \in \mathbb{C}[t]$$

where the product is over all primitive nth roots of unity $\varepsilon \in \mathbb{C}$.

As exercises, one proves the following two propositions.

Proposition 15.1. *For $n \in \mathbb{Z}_+$, the primitive nth roots of unity in $\mathbb{C}$ are $\mathrm{e}^{2\pi i k/n}$ where $k \in \mathbb{Z}$ with hcf$(k,n) = 1$. Thus with $\zeta = \mathrm{e}^{2\pi i/n}$,*

$$\{\zeta^k : \ 1 \leq k \leq n, \ \textit{hcf}(k,n) \ \}$$

is the set of primitive nth roots of unity in $\mathbb{C}$. Hence

$$\deg \Phi_n = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

where $(\mathbb{Z}/n\mathbb{Z})^\times$ *is the group of units of the ring* $\mathbb{Z}/n\mathbb{Z}$.

Proposition 15.2. *For* $n \in \mathbb{Z}_+$, $t^n - 1 = \prod_{d|n} \Phi_d$. *Hence*

$$n = \sum_{d|n} \phi(d)$$

where $\phi(d) = |(\mathbb{Z}/d\mathbb{Z})^\times|$.

The above proposition gives a recursive way of defining the cyclotomic polynomials:

$$\begin{aligned}
\Phi_1 &= t - 1, \\
\Phi_2 &= (t^2 - 1)/\Phi_1 = t + 1, \\
\Phi_3 &= (t^3 - 1)/\Phi_1 = t^2 + t + 1, \\
\Phi_4 &= (t^4 - 1)/(\Phi_1\Phi_2) = t^2 + 1, \\
\Phi_5 &= (t^5 - 1)/\Phi_1 = t^4 + t^3 + t^2 + t + 1, \\
\Phi_6 &= (t^6 - 1)/(\Phi_1\Phi_2\Phi_3) = t^2 - t + 1,
\end{aligned}$$

and so on. Note that when p is prime, $\Phi_p = (t^p - 1)/\Phi_1 = t^{p-1} + t^{p-2} + \cdots + t + 1$.

Proposition 15.3. *For* $n \in \mathbb{Z}_+$, $\Phi_n \in \mathbb{Z}[t]$.

Proof. We argue by induction on n.

Clearly $\Phi_1 \in \mathbb{Z}[t]$.

Now suppose that $n > 1$, and that for $1 \leq d < n$ we have $\Phi_d \in \mathbb{Z}[t]$. Recall that by Proposition 15.1, we have

$$t^n - 1 = \prod_{d|n} \Phi_d.$$

Thus with $m = \deg \Phi_n$, we can write

$$\prod_{\substack{d|n \\ d<n}} \Phi_d = \sum_{i=0}^{n-m} a_i t^{n-m-i} \text{ and } \Phi_n = \sum_{j=0}^{m} b_j t^{m-j}.$$

By hypothesis, $a_i \in \mathbb{Z}$ for each i for each $d < n$. Since each Φ_d is monic, we have $a_0 = 1$. So

$$\begin{aligned}
t^n - 1 &= \sum_{i=0}^{n-m} \sum_{j=0}^{m} a_i b_j t^{n-i-j} \\
&= \sum_{k=0}^{n} \sum_{i=0}^{k} a_i b_{k-i} t^{n-k}.
\end{aligned}$$

Note that for each k,

$$\sum_{i=0}^{k} a_i b_{k-i} \in \mathbb{Z}$$

since $t^n - 1 \in \mathbb{Z}[t]$.

Now we argue by induction on k to show that (with n fixed) we have $b_0, b_1, \ldots, b_n \in \mathbb{Z}$. With $k = 0$ we have $b_0 = a_0 b_0 \in \mathbb{Z}$. So suppose that $0 < k \leq n$ and $b_0, \ldots, b_{k-1} \in \mathbb{Z}$. Again using that $a_0 = 1$, we have

$$b_k + \sum_{i=1}^{k} a_i b_{k-i} = \sum_{i=0}^{k} a_i b_{k-i} \in \mathbb{Z},$$

so using our induction hypothesis we have $b_k \in \mathbb{Z}$. Thus by induction on k, we have $b_k \in \mathbb{Z}$ for each k.

Hence by induction on n, we have $\Phi_n \in \mathbb{Z}[t]$ for all $n \in \mathbb{Z}_+$. □

Proposition 15.4. *For $n \in \mathbb{Z}_+$, Φ_n is irreducible over $\mathbb{Q}$.*

Proof. For the sake of contradiction, suppose Φ_n is reducible over $\mathbb{Q}$. Thus Φ_n has an irreducible factor $q \in \mathbb{Q}[t]$, and scaling q as necessary, we can assume q is a primitive element of $\mathbb{Z}[t]$. Hence $\Phi_n = qr$ where $r \in \mathbb{Z}[t]$ and $\deg q, \deg r \geq 1$. Since Φ_n is monic, we have that the leading coefficients of q and r are ± 1, so again by scaling as necessary, we can assume that q, r are monic elements of $\mathbb{Z}[t]$.

Let $\varepsilon, \zeta \in \mathbb{C}$ be roots of q, r (respectively). Since q is monic and irreducible over $\mathbb{Q}$, we have $q = m_\varepsilon(\mathbb{Q})$. Also, as ε, ζ are roots of Φ_n, they are primitive nth roots of unity, and $\varepsilon \neq \zeta$ since $qr = \Phi_n$ has no multiple roots. Hence $\zeta = \varepsilon^k$ for some $k > 1$. We choose ε, ζ so that k is as small as possible. Take p to be a prime divisor of k. Since $\zeta = \varepsilon^k$ has order n, we must have that $p \nmid n$. Hence ε^p is a primitive nth root of unity (and thus is a root of Φ_n). Also, $(\varepsilon^p)^{k/p} = \zeta$, so by the choice of ε, ζ, we cannot have that ε^p is a root of q. Hence ε^p must be a root of r. By our choice of k, we must have $p = k$. Further, $q(t)$ must divide $r(t^p)$ since ε is a root of $r(t^p)$ and $q = m_\varepsilon(\mathbb{Q})$. Thus $r(t^p) = q(t)s(t)$ for some $s \in \mathbb{Q}[t]$. Since q, r are monic, an argument as in the proof of the previous proposition shows that $s \in \mathbb{Z}[t]$.

With $r(t) = t^k + a_{k-1}t^{k-1} + \cdots + a_0 \in \mathbb{Z}[t]$, we have

$$(r(t))^p \equiv t^{pk} + a_{k-1}p^{p(k-1)} + \cdots + a_0 \equiv r(t^p) \pmod{p}.$$

Therefore $(r(t))^p \equiv q(t)s(t) \pmod{p}$. We know that $\mathbb{Z}/p\mathbb{Z}[t]$ is a UFD, and $\deg(q(t) \bmod p) = \deg q(t) > 1$, so there is some $h(t) \in \mathbb{Z}[t]$ so that, in $\mathbb{Z}/p\mathbb{Z}[t]$, $h(t)$ is an irreducible divisor of $q(t)$ and hence of $r(t)$. Thus modulo p, $(h(t))^2$ divides $\Phi_n(t) = q(t)r(t)$. Hence modulo p, $\Phi_n(t)$ has a multiple root. Thus modulo p, $t^n - 1$ has a multiple root, as $\Phi_n(t)$ divides $t^n - 1$. But $nt^{n-1} \not\equiv 0 \pmod{p}$, so by Theorem 8.1, $t^n - 1$ does not have a multiple modulo p, a contradiction.

Hence $\Phi_n(t)$ must be irreducible over $\mathbb{Q}$. □

Notation. For $n \in \mathbb{Z}_+$, let $\mathbb{Q}_n = \mathbb{Q}(\varepsilon)$ where $\varepsilon \in \mathbb{C}$ is a primitive nth root of unity.

As an exercise, one proves the following.

Proposition 15.5. *Fix $n \in \mathbb{Z}$ with $n > 1$. Then $\mathbb{Q}_n : \mathbb{Q}$ is a Galois extension, and $Gal(\mathbb{Q}_n : \mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.*

The proof of the next result uses Dirichlet's Theorem on primes in arithmetic progressions, which states that for any $n, m \in \mathbb{Z}_+$ with $\mathrm{hcf}(n, m) = 1$,

there exist infinitely many primes p so that $p \equiv m \pmod{n}$. (When $m = 1$, this can be proved using cyclotomic polynomials; see, for instance, section 7.7 of Grillet's book *Algebra*.)

Theorem 15.6. *Every finite abelian group is the Galois group of some Galois extension of* $\mathbb{Q}$.

Proof. Let G be a finite abelian group. From Group Theory we know that G is isomorphic to $C_{n_1} \times C_{n_2} \times \cdots \times C_{n_s}$ where $n_i \in \mathbb{Z}$ with $n_i > 1$ and $C_{n_i} \simeq (\mathbb{Z}/n_i\mathbb{Z})^\times$. By Dirichlet's Theorem, there are distinct primes $p_1, \ldots, p_s$ so that $p_i \equiv 1 \pmod{n_i}$ $(1 \le i \le s)$. Set $n = p_1 \cdots p_s$; so $\mathbb{Q}_n : \mathbb{Q}$ is a Galois extension with $Gal(\mathbb{Q}_n : \mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. From Group Theory we know that for $k, m \in \mathbb{Z}_+$ with $\mathrm{hcf}(k, m) = 1$, we have $(\mathbb{Z}/km\mathbb{Z})^\times \simeq (\mathbb{Z}/k\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$. Thus there is an isomorphism

$$\psi : (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s\mathbb{Z})^\times \to Gal(\mathbb{Q}_n : \mathbb{Q}).$$

For each i, $(\mathbb{Z}/p_i\mathbb{Z})^\times$ is cyclic [recall that p_i is prime] and $n_i | (p_i - 1)$; thus $(\mathbb{Z}/p_i\mathbb{Z})^\times$ has a cyclic (and hence abelian) subgroup H_i of order $(p_i - 1)/n_i$. Hence $(\mathbb{Z}/n\mathbb{Z})^\times$ has a subgroup $H \simeq H_1 \times \cdots \times H_s$. Let $F \subseteq \mathbb{Q}_n$ be the fixed field of $\psi(H)$. Since H is a normal subgroup, so is $\psi(H)$, and $F : \mathbb{Q}$ is a Galois extension with $Gal(F : \mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times / H$. Finally, note that

$$(\mathbb{Z}/n\mathbb{Z})^\times / H \simeq (\mathbb{Z}/p_1\mathbb{Z})^\times / H_1 \times \cdots \times (\mathbb{Z}/p_s\mathbb{Z})^\times / H_s \simeq C_{n_1} \times \cdots \times C_{n_s}.$$

So $Gal(F : \mathbb{Q}) \simeq G$. □

16. Cyclic extensions and Abel's Theorem

Definition. We say an extension $L : K$ is cyclic if $L : K$ is a Galois extension and $Gal(L : K)$ is a cyclic group.

Proposition 16.1. *Suppose that* $t^n - \theta \in K[t]$ *where* $n \in \mathbb{Z}_+$ *and that* $\mathrm{char}K$ *does not divide* n. *Let* $L : K$ *be a splitting field extension for* $t^n - \theta$. *Then for some primitive* n*th root of unity* ε, *we have* $\varepsilon \in L$. *Also,* $L : K(\varepsilon)$ *is a cyclic extension,* $|Gal(L : K(\varepsilon))|$ *divides* n, *and* $t^n - \theta$ *is irreducible over* $K(\varepsilon)$ *if and only if* $|Gal(L : K(\varepsilon))| = n$.

Proof. Since $\mathrm{char}K \nmid n$, we know by Theorem 8.1 that $f = t^n - \theta$ is separable over K. Assume $K \subseteq L$, and let $\alpha_1, \ldots, \alpha_n \in L$ be the roots of f (which are necessarily distinct as $Df \neq 0$ and hence by Theorem 8.1, f has no repeated roots). Thus for $1 \le j \le n$, we have $(\alpha_1 \alpha_j^{-1})^n = 1$, and hence $\alpha_1\alpha_1^{-1}, \alpha_1\alpha_2^{-1}, \ldots, \alpha_1\alpha_n^{-1}$ are n distinct nth roots of unity that lie in L. So for some j, $\varepsilon = \alpha_1\alpha_j^{-1}$ is a primitive nth root of unity, and with $\alpha = \alpha_1$,

$$t^n - \theta = (t - \alpha)(t - \varepsilon\alpha) \cdots (t - \varepsilon^{n-1}\alpha).$$

Thus $L = K(\varepsilon, \alpha)$.

Take $\sigma \in Gal(L : K(\varepsilon))$. So σ is determined by its action on α, and $\sigma(\alpha) = \varepsilon^{j(\sigma)}\alpha$ for some $j(\sigma) \in \mathbb{Z}$, $0 \le j(\sigma) < n$. Define $\psi : Gal(L : K(\varepsilon)) \to \mathbb{Z}/n\mathbb{Z}$ by $\psi(\sigma) = j(\sigma) + n\mathbb{Z}$. Write $\overline{j(\sigma)}$ for $j(\sigma) + n\mathbb{Z}$. One easily checks that for $\tau, \sigma \in Gal(L : K(\varepsilon))$, we have $\psi(\tau \circ \sigma) = \psi(\tau) + \psi(\sigma)$. Also, $\ker \psi = \overline{0}$,

so ψ is injective. Hence $Gal(L : K(\varepsilon))$ is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$, which is necessarily cyclic [as $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group]. Also, by Lagrange's Theorem, the order of $Gal(L : K(\varepsilon))$ divides n.

Since $L : K(\varepsilon)$ is Galois and $L = K(\varepsilon, \alpha)$, we know that

$$|Gal(L : K(\varepsilon))| = [L : K(\varepsilon)] = \deg m_\alpha(K(\varepsilon)).$$

Also, $m_\alpha(K(\varepsilon))$ divides $t^n - \theta$, so $\deg m_\alpha(K(\varepsilon)) = n$ if $t^n - \theta$ is irreducible over $K(\varepsilon)$, and otherwise $\deg m_\alpha(K(\varepsilon)) < n$. □

Theorem 16.2. *(Abel's Theorem) Suppose q is a prime, char$K \neq q$, and $\theta \in K^\times$. Then either $t^q - \theta$ is irreducible over K or $t^q - \theta$ has a root in K. In the latter case, $t^q - \theta$ splits over K if and only if K contains a primitive qth root of unity.*

Proof. Note that since char$K \neq q$, by Theorem 8.1 $t^q - \theta$ is separable over K.

If $t^q - \theta$ is irreducible over K then we are done. So suppose $t^q - \theta$ is reducible over K. Let $L : K$ be a splitting field extension for $t^q - \theta$, and let g be a monic factor of $t^q - \theta$ that is irreducible over K. Hence g splits over L. With $\beta \in L$ a root of g, we have that β is a root of $t^q - \theta$. By Proposition 16.1, we know that there is some $\varepsilon \in L$ so that ε is a primitive nth root of unity. So $\beta, \beta\varepsilon, \beta\varepsilon^2, \ldots, \beta\varepsilon^{q-1}$ are the distinct roots of $t^q - \theta$ in L. Hence with $d = \deg g$, there are $m_2, \ldots, m_d \in \mathbb{Z}_+$ so that in $L[t]$, we have

$$g = (t - \beta)(t - \beta\varepsilon^{m_2}) \cdots (t - \beta\varepsilon^{m_d}).$$

Since $g \in K[t]$, we have $\beta^d\varepsilon^m \in K$ where $m = m_2 + \cdots + m_d$. Since $g \neq t^q - \theta$, we have $0 < d = \deg g < q$. Since q is prime, this means that there is some $d' \in \mathbb{Z}_+$ so that $dd' = 1 + q\ell$ for some $\ell \in \mathbb{Z}_+$. Thus

$$\beta\theta^\ell\varepsilon^{md'} = (\beta^d\varepsilon^m)^{d'} \in K.$$

Since $\theta \in K^\times$, we have $\beta\varepsilon^{md'} \in K$, and we know that $\beta\varepsilon^{md'}$ is one of the roots of $t^q - \theta$.

Suppose still that $t^q - \theta$ is reducible over K. Assume that $K \subseteq \overline{K}$. Take $\alpha \in K$ and $\varepsilon \in \overline{K}$ so that $\alpha^q = \theta$ and ε is a primitive qth root of unity. Then over $\overline{K}$,

$$t^q - \theta = (t - \alpha)(t - \varepsilon\alpha) \cdots (t - \varepsilon^{q-1}\alpha).$$

So $t^q - \theta$ splits over K if and only if $\alpha, \varepsilon\alpha, \ldots, \varepsilon^{q-1}\alpha \in K$, and this occurs if and only if $\varepsilon = \alpha^{-1}\varepsilon\alpha \in K$. □

17. Solvability and solubility

Definition. A finite group G is *soluble* if there is a series of groups

$$\{\mathrm{id}\} = G_0 \leq G_1 \leq \ldots \leq G_n = G,$$

with the property that $G_i \trianglelefteq G_{i+1}$ and G_{i+1}/G_i is abelian $(0 \leq i < n)$.

So abelian groups are soluble. Fact: the smallest insoluble group is A_5 (having order 60).

Theorem 17.1. *Let K be a field of characteristic zero. Then $f \in K[x]$ is soluble by radicals if and only if $Gal_K(f)$ is soluble.*

We will prove only one direction of this theorem, namely that whenever $f \in K[x]$ is soluble by radicals, then $\mathrm{Gal}_K(f)$ is soluble.

Lemma 17.2. *Suppose char$(K) = 0$ and $L : K$ is a radical extension. Then there exists an extension $N : L$ such that $N : K$ is normal and radical.*

Proof. One has $L = K(\alpha_1, \ldots, \alpha_n)$, where for $1 \leq i \leq n$ one has

$$\alpha_i^{r_i} \in K(\alpha_1, \ldots, \alpha_{i-1}).$$

Note that there is no loss of generality in supposing that each r_i is a prime number. Let $N : L$ be a splitting field extension for

$$\prod_{i=1}^{n} m_{\alpha_i, K}.$$

Then $N : L : K$ is a tower of extensions with $N : K$ normal. Moreover, one has

$$N = K\left(\{\sigma(\alpha_j) : \sigma \in \mathrm{Gal}(N : K) \text{ and } 1 \leq j \leq n\}\right),$$

since $\mathrm{Gal}(N : K)$ is transitive on the roots of each $m_{\alpha_i, K}$. But

$$(\sigma(\alpha_j))^{r_j} = \sigma(\alpha_j^{r_j}) \in K(\alpha_1, \ldots, \alpha_{j-1}),$$

since $\alpha_j^{r_j} \in K(\alpha_1, \ldots, \alpha_{j-1})$. Thus $\sigma(\alpha_j)$ is radical over K for each j and $\sigma \in \mathrm{Gal}(N : K)$, whence $N : K$ is radical. □

Definition. We say that an extension $L : K$ is cyclic if $L : K$ is a Galois extension and $\mathrm{Gal}(L : K)$ is a cyclic group.

Lemma 17.3. *Let char$(K) = 0$ and let p be a prime number. Also, let $L : K$ be a splitting field extension for $x^p - 1$. Then Gal$(L : K)$ is cyclic.*

Proof. Let $L = K(\omega)$, where ω is a primitive p-th root of 1. Let g be a primitive root modulo p, and define $\sigma \in \mathrm{Gal}(L : K)$ as the map taking ω to ω^g. Note that $\mathrm{Gal}(L : K)$ is defined by its action on powers of ω, and that an element $\tau \in \mathrm{Gal}(L : K)$ maps ω to some other root of unity $\omega_1 = \omega^a$, for some integer a with $0 \leq a < p$. But $a \equiv g^r \pmod{p}$ for a suitable integer r, and then $\tau = \sigma^r$. Thus we see that $\mathrm{Gal}(L : K) = \langle \sigma \rangle$, and that $\mathrm{Gal}(L : K)$ is cyclic. □

Lemma 17.4. *Let char$(K) = 0$ and suppose that n is an integer such that $x^n - 1$ splits in K. Let $L : K$ be a splitting field extension for $x^n - a$, for some $a \in K$. Then Gal$(L : K)$ is abelian.*

Proof. Let $\alpha \in L$ be a root of $x^n - a$, so $L = K(\alpha)$. If $\sigma, \tau \in \mathrm{Gal}(L : K)$, we have $\sigma(\alpha) = \omega_1 \alpha$ and $\tau(\alpha) = \omega_2(\alpha)$, for some $\omega_1, \omega_2 \in K$ with $\omega_1^n = \omega_2^n = 1$. Then

$$\sigma\tau(\alpha) = \omega_2\omega_1\alpha = \omega_1\omega_2\alpha = \tau\sigma(\alpha),$$

so that σ and τ commute. Thus we see that $\mathrm{Gal}(L : K)$ is indeed abelian. □

Theorem 17.5. *Let char$(K) = 0$ and let $L : K$ be Galois. Suppose that there is an extension $M : L$ such that $M : K$ is radical. Then Gal$(L : K)$ is soluble.*

Proof. Lemma 17.3 shows that there is no loss of generality in supposing $M : K$ to be normal and hence Galois. So we only need to show that $\mathrm{Gal}(M : K)$ is soluble (since any subgroup of a soluble group is also soluble).

Write $M = K(\alpha_1, \ldots, \alpha_n)$ with $\alpha_i^{r_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ and r_i prime for each i. We proceed by induction. If $n = 1$ and $\alpha_1 \in K$, then we are trivially done. Then we may suppose that $\alpha_1 \notin K$, and that p is a prime for which $\alpha_1^p = a \in K$. Let $\Sigma : K$ be a splitting field extension of $x^p - a$ over K, so $\Sigma = K(\alpha_1, \omega)$, where ω is a primitive p-th root of 1. Then we find that

$$\Sigma : K(\omega) \text{ is Galois with abelian Galois group (Lemma 17.4),}$$

$$K(\omega) : K \text{ is Galois with abelian Galois group (Lemma 17.3).}$$

Then the Fundamental Theorem of Galois Theory shows that

$$\{\mathrm{id}\} \trianglelefteq \mathrm{Gal}(\Sigma : K(\omega)) \trianglelefteq \mathrm{Gal}(\Sigma : K)$$

with

$$\mathrm{Gal}(K(\omega) : K) \cong \mathrm{Gal}(\Sigma : K)/\mathrm{Gal}(\Sigma : K(\omega)).$$

Notice that the left hand side is an abelian group, and hence $\mathrm{Gal}(\Sigma : K)$ is soluble. This completes the proof of the inductive hypothesis when $n = 1$. On noting that $M = \Sigma(\alpha_2, \ldots, \alpha_n)$, we may proceed in like manner inductively to show that $\mathrm{Gal}(M : \Sigma)$ is soluble. Moreover,

$$\mathrm{Gal}(M : K)/\mathrm{Gal}(M : \Sigma) \cong \mathrm{Gal}(\Sigma : K),$$

so that $\mathrm{Gal}(M : K)$ is soluble (a consequence of Group Theory: if $N \trianglelefteq G$, then G is soluble if and only if both N and G/N are soluble). This completes the proof. □

We finish by proving showing that there exists a quintic polynomial defined over $\mathbb{Q}$ having insoluble Galois group, and hence insoluble by radicals. To see this, consider the polynomial $f(x) = x^5 - 4x + 2$. This polynomial is irreducible over $\mathbb{Q}$, as a consequence of Eisenstein's theorem using the prime 2. Moreover, since $f'(x) = 5x^4 - 4$, one sees that f has 3 real roots and 2 complex roots (observe that $f(-2) = -22$, $f(0) = 2$, $f(1) = -1$, $f(2) = 26$). Then $\mathrm{Gal}_{\mathbb{Q}}(f)$ contains a transposition (fixing the real roots and interchanging the 2 complex roots by conjugation). Then since there are 5 roots (an odd prime number of roots), and $\mathrm{Gal}_{\mathbb{Q}}(f)$ is isomorphic to a subgroup of S_5, it follows that in fact $\mathrm{Gal}_{\mathbb{Q}}(f)$ is isomorphic to the whole of S_5 (the group of permutations on 5 symbols). But S_5 contains the insoluble subgroup A_5, and hence is itself insoluble. We therefore conclude that $\mathrm{Gal}_{\mathbb{Q}}(f)$ is insoluble, and hence that $f(x) = 0$ cannot be solved by using radical extensions of $\mathbb{Q}$.