GALOIS THEORY

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

The notes are organised into the following sections.

§0. Introduction
§1. Field extensions and algebraic elements: an enhanced review
§2. Ruler and compass constructions: an enhanced review
§3. Extending field homomorphisms and the Galois group of an extension
§4. Algebraic closures
§5. Splitting field extensions
§6. Normal extensions and compositums
§7. Separability
§8. Inseparable polynomials, differentiation, and the Frobenius map
§9. The Primitive Element Theorem
§10. Fixed fields and Galois extensions
§11. The main theorems of Galois theory
§12. Finite fields
§13. Solvability by radicals: quadratic, cubic, and quartic polynomials
§14. Higher degree polynomials and Hilbert's 13th Problem (non-examinable)
§15. Cyclotomic polynomials and cyclotomic extensions
§16. Cyclic extensions and Abel's Theorem
§17. Solvability and solubility (non-examinable)

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.

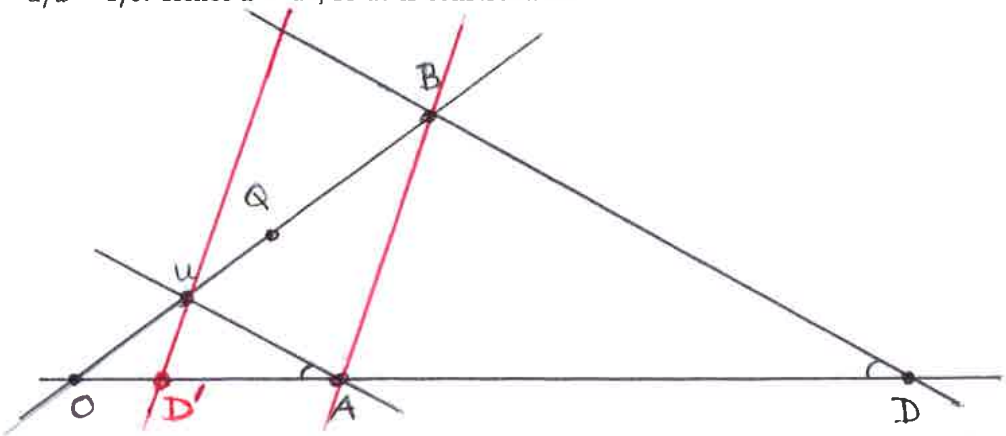
Proof. One shows as an exercise that $a + b$ is constructible.

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.] $\square$

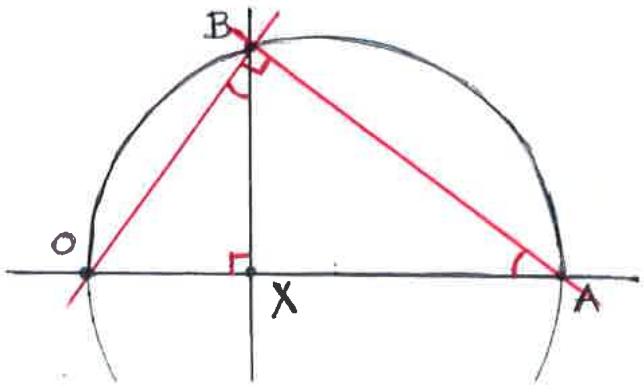
Suppose that $a, b \in \mathbb{R}_+$ are constructible. We show that ab, a/b, $\sqrt{a}$ are also constructible:

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). Sinc 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 $\alpha \in L$. 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 implies that for $f \in K[t]$ and $\sigma \in Gal(L : K)$, σ permutes the roots of f that lie in L; we show this in the proof of the following theorem.

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

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

Since $L[t]$ is a UFD, any (nonzero) element of $K[t]$ has finitely many roots in L. Thus R is a finite subset of L. Consider the (finite) set $\sigma(R) = \{\sigma(\beta) : \beta \in R\ \}$. As σ is injective [since every field homomorphism is injective], we know that R and $\sigma(R)$ have the same (finite) number of elements. Also, by Lemma 3.1, every element of $\sigma(R)$ is a root of $m_\alpha(K)$, so we must have $R = \sigma(R)$. Hence for some $\beta \in R$, we have $\sigma(\beta) = \alpha$. As this argument holds for all $\alpha \in L$, we have that σ maps L onto 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 $i \in \mathcal{I} \setminus \mathcal{J}$. 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 $f \in E_{n-1}[t] \setminus E_{n-1}$. So each E_n is algebraic over K. Hence $\overline{K} = \cup_{n\in\mathbb{Z}_+} E_n$ is algebraic over K. Suppose $f \in \overline{K}[t] \setminus \overline{K}$. 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 $f \in K[t] \setminus K$. 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 $S \subseteq K[t] \setminus K$ 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 $f \in K[t] \setminus K$ (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 $f \in K[t] \setminus K$. 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

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

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.