GALOIS THEORY

Notes by L.H. Walling

Table of Contents

0. Introduction

In Galois Theory, we will look at algebraic field extensions $L : K$. For simplicity of our discussion here, let us suppose $L : K$ is an algebraic field extension with $K \subseteq L$. We consider the actions of automorphisms σ of L that leave K pointwise fixed; we will see that for $\alpha \in L$, such an automorphism σ maps α to another root of $m_\alpha(K)$, the minimal polynomial for α over K.

Example. Consider the "imaginary" number $i \in \mathbb{C}$. We describe i as a root of the polynomial $t^2 + 1$, an irreducible polynomial in $\mathbb{Q}[t]$. But $-i$ is also a root of $t^2 + 1$, and complex conjugation is an automorphism of $\mathbb{Q}(i)$ that takes i to $-i$, leaving $\mathbb{Q}$ pointwise fixed. (Recall that $\mathbb{Q}(i)$ denotes the smallest subfield of C containing $\mathbb{Q}$ and i.) So algebraically, how do we distinguish i from $-i$?

Suppose again $L : K$ is an algebraic field extension with $K \subseteq L$. Also suppose $\alpha \in K$ so that all the roots of $m_\alpha(K)$ lie in L. (Recall that since L is a field, $L[t]$ is a unique factorisation domain.) Let $Gal(L : K)$ denote the set of all automorphisms of L that leave K pointwise fixed; we will see this is a group. We will also see that when $L : K$ is a "Galois extension" (as defined in Section 10), $Gal(L : K)$ permutes the roots of $m_\alpha(K)$, and in fact this group $Gal(L : K)$ acts transitively on the roots of $m_\alpha(K)$ (so in some sense, $Gal(L : K)$ can't distinguish between the roots of $m_\alpha(K)$).

The Fundamental Theorem of Galois Theory shows (among other things) that when $L : K$ is a finite Galois extension, there is a one-to-one correspondence between subgroups of $Gal(L : K)$ and fields M with $K \subseteq M \subseteq L$. This might seem surprising, as in this setting, $Gal(L : K)$ is a finite group, yet L can be an infinite set, yet we find there are only finitely many of these "intermediate" fields M. This is a beautiful and closely woven theory.

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 Axiom of Choice, and hence assume Zorn's Lemma.

Zorn's Lemma: Suppose M is a nonempty, partially ordered set with $\leq$ denoting the partial ordering. A chain C in M is a (non-empty) collection of elements $\{a_i\}_{i \in I}$ of M 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 M has an upper bound in M; then M has a maximal element m, meaning that if $b \in M$ 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. *Suppose R is a commutative ring with unity, and A a proper ideal of R. Then A 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 $C = \{J_i\} i \in \mathcal{I}$ 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

Recall that with R, R' commutative rings with unity (where "unity" means a multiplicative identity), a map $\varphi : R \to R'$ 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) $\varphi(1) = 1$.

Suppose that K is a field. Recall that this means K is a commutative ring with unity, denoted by 1, so that

(1) $1 \neq 0$ where 0 denotes the additive identity in K;
(2) for every $\alpha \in K$ with $\alpha \neq 0$, there is a (unique) $\alpha^{-1} \in K$ so that $\alpha \cdot \alpha^{-1} = 1$.

As 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.*

Proof. We know that the $\ker \varphi$ is an ideal of the domain. In this case, since K is a field, the ideals of K are $\{0\}$ and K. Since $\varphi(1) = 1$ and $1 \neq 0$, we cannot have $1 \in \ker \varphi$. Hence $\ker \varphi \neq K$, leaving us with $\ker \varphi = \{0\}$. Hence [from another result from Algebra 2], φ is injective. □

Definitions. 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 (relative to the embedding φ). When K, L are fields with $K \subseteq L$, we assume $\varphi : K \to L$ is the identity map on K. With $L : K$ a field extension (relative to the embedding $\varphi : K \to L$), and $\alpha \in L$, we say α is algebraic over K if α is a root of $\varphi(f)$ for some polynomial $f \in K[t] \setminus K$. (Here we extend $\varphi : K \to L$ to an injective homomorphism $\varphi : K[t] \to L[t]$ by setting $\varphi(t) = t$.) We say $L : K$ is an algebraic extension if each element of L is algebraic over 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 $L : M : K$ is a tower of field extensions if $L : M$ and $M : K$ 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 $L : M : K$ is a tower of field extensions. Then $M : K$ is a field extension, and*

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

Further, R

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

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

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

is a basis for L over K.

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

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

□

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

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. Further, for $f \in I$, in $L[t]$ we have $f = (t - \alpha)q$ for some $q \in L[t]$.

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 $g = h$.

Now say $f \in I$. Since $L[t]$ is a Euclidean domain, there are $q, r \in L[t]$ so that $f = (t - \alpha)q + r$ where $r = 0$ or $\deg r < \deg(t - \alpha)$ (meaning $r \in L$). As $f(\alpha) = 0$ we must have $r = 0$ and so $f = (t - \alpha)q$. □

Definition. Suppose that $L : K$ is a field extension, and $\alpha \in L$ so that α is algebraic over K. When $K \subseteq L$, the minimal polynomial for α over K is the unique monic irreducible polynomial in $K[t]$ for which α is a root. When $L : K$ is a field extension relative to a homomorphism $\varphi : K \to L$, then the minimal polynomial for α over K is the unique monic irreducible polynomial in $\varphi(K)[t]$ for which α is a root.

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. □

The proof of the following theorem depends crucially on the facts that

(i) with R a commutative ring with unity, and I an ideal of R, then R/I is a field if and only if I is a maximal ideal, and
(ii) with K a field and $f \in K[t] \setminus K$, the ideal (f) in $K[t]$ is a maximal ideal if and only if f is irreducible in K.

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 $\alpha_1, \ldots, \alpha_n$).*
(iii) *There are $\alpha_1, \ldots, \alpha_n \in L$ so that $\alpha_1, \ldots, \alpha_n$ are algebraic over K and $L = K(\alpha_1, \ldots, \alpha_n)$.*

As exercises, one also proves the following.

Theorem 1.15. *Suppose that $L : M : K$ is a tower of field extensions, and (by associating K with its isomorphic image in M, and M with its isomorphic image in L) assume that $K \subseteq M \subseteq L$. Then $L : K$ is an algebraic extension if and only if $L : M$ and $M : K$ are algebraic extensions.*

Proposition 1.16. *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 $\mathrm{char}K$, 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 1.17. *Suppose K is a field.*

(a) *Suppose $charK > 0$; then $charK$ is prime.*
(b) *Suppose $charK = p > 0$; 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 $n = \mathrm{char}K$. 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 $\mathrm{char}K$, 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 1.18. *Suppose K is a field and $charK = p > 0$. 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 1.19. *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 $\operatorname{ord}(y) | \operatorname{ord}(x)$. Let $k = \operatorname{ord}(x)$; so by Lagrange's Theorem, $k|n$ and hence $k \leq n$. Also, for all $y \in G$, we have $\operatorname{ord}(y)|k$ 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 $c = \operatorname{hcf}(a_0, \ldots, a_n)$ 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 $f = a_0 + a_1 M + \cdots + a_n M^n \in R[M]$ with $f \neq 0$. We define the content of f to be $\operatorname{hcf}(a_0, \ldots, a_n)$. We say $f \in R[M]$ is primitive if $f \neq 0$ and the content of f is 1.

Theorem 1.20. *(Gauss' Lemma) Suppose R is a UFD, Q its field of fractions. Suppose f is a primitive element of $R[M]$ with $\deg f > 0$. Then f is irreducible in $R[M]$ if and only if f is irreducible in $Q[M]$.*

Theorem 1.21. *(Eisenstein's Criterion) Suppose R is a UFD, $f = a_0 + a_1 M + \cdots + a_n M^n \in R[M]$ 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 $R[M]$ (and hence f is irreducible in $Q[M]$ where Q is the field of fractions of R).*

Theorem 1.22. *Let R be an integral domain, and I a prime ideal of R. Define $\varphi : R[M] \to (R/I)[M]$ by*

$$\varphi(a_0 + a_1 M + \cdots + a_n M^n) = \overline{a}_0 + \overline{a}_1 M + \cdots + \overline{a}_n M^n$$

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

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 M.

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.

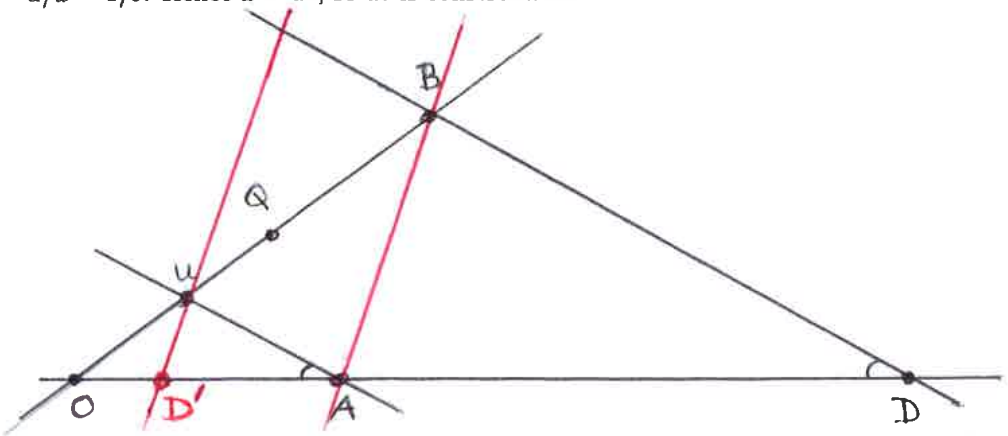
To show $ab, a/b$ are constructible, it suffices to consider the case where $b > 0$. Then, to construct ab and a/b, we begin with a line segment OA of length a; fix a point Q not on the line through O and A. On the line through O and Q, fix points U and B so that the length of the segment OU is 1, and 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 M so that the distance from M 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 M that is perpendicular to the line through O and M. Let B be a point where L intersects the circle, and let x denote the distance from M 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 $\angle BOM$ (which is the same as $\angle BOA$), triangles $\triangle OBA$ and $\triangle OMB$ are similar. Hence $\angle OAB$ is equal to $\angle OBM$. Also, $\angle OAB$ is the same as $\angle MAB$, so the triangles $\triangle MAB$ and $\triangle MBO$ 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.] $\square$

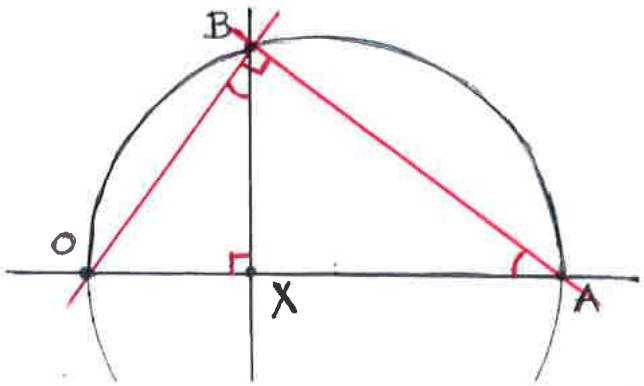
Suppose that $a, b \in \mathbb{R}_+$ are constructible. We show that ab, a/b, $\sqrt{a}$ are also constructible:

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 $P_0 = O$, $P_1 = M$, $P_n = P$, 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

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

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

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

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

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

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

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

and of

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

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

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

First suppose $u \neq 0$. Then by solving $uM + vY + w = 0$ for M 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 M 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

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

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

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

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 M; 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 M. 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 M. Let L be the line through A perpendicular to the line through O and M, and let B_1 be a point where L intersects the circle. Then the arc on the circle between M 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 M to B_1, B_{n-1} to M, 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 $f \in K[t] \setminus K$ and $\alpha \in L$. We have that $f(\alpha) = 0$ if and only if $f(\tau(\alpha)) = 0$.*

Note that when $L : K$ is a field extension relative to a homomorpism $\varphi : K \to L$, in the above proposition we replace $f \in K[t]$ by $\varphi(f) \in \varphi(K)[t]$ (so $\varphi(f)(\alpha) = 0$ if and only if $\varphi(f)(\tau(\alpha)) = 0$).

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.*

(a) *Take $f \in K_1[t] \setminus K_1$. Then f is irreducible over K_1 if and only if $\sigma(f)$ is irreducible over K_2.*
(b) *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. (a) This is left as an exercise (and was proved in Algebra 2).

(b) 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

verifies 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

$$\begin{aligned}\ker \varphi\circ\sigma &= \{g \in K_1[t] :\ \sigma(g) + (f_2) = 0 + (f_2)\ \}\\ &= \{g \in K_1[t] :\ \sigma(g) \in (f_2)\ \}\\ &= \{g \in K_1[t] :\ \sigma(g) = f_2h_2 \text{ for some } h_2 \in K_2[t]\ \}\\ &= \{g \in K_1[t] :\ g = \sigma^{-1}(f_2h_2) \text{ for some } h_2 \in K_2[t]\ \}\\ &= \{g \in K_1[t] :\ g \in f_1\sigma^{-1}(K_2[t])\ \}\\ &= (f_1)\end{aligned}$$

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 with $\tau = \psi_2 \circ \omega \circ \psi_1^{-1}$, we have $\tau : K_1(\alpha) \to K_2(\beta)$ is an isomorphism. Diagrammatically, we have

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

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 $c \in K_1$, $\psi_2 \circ \omega \circ \psi_1^{-1}(c) = \psi_2 \circ \omega(c + (f_1)) = \psi_2(\sigma(c) + (f_2)) = \sigma(c)$. 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; assume $K \subseteq L$ and $\sigma : L \to L$ is a K-homomorphism. Then σ is an automorphism of L.*

Proof. 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 element of $K[t] \setminus K$ 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 Proposition 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 $\sigma \in Aut(L)$.

(How do we modify this proof if $L : K$ is an extension relative to a homomorphism $\varphi : K \to L$?) □

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 $\sigma_{i-1} : K_{i-1} \to L$. (Note that by Theorem 3.4, such a homomorphism $\psi : L \to L$ is actually an isomorphism as any finite extension is an algebraic extension.)*

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) *For any algebraic extension $L : M$ relative to a homomorphism $\varphi : M \to L$, φ is an isomorphism.*

Discussion. Suppose $L : M$ and $M : K$ are algebraic field extensions (not necessarily of finite degrees); assume $K \subseteq M \subseteq L$. We want to show that $L : K$ is an algebraic extension; for this, choose $\alpha \in L$. Then α is the root of a (nonzero) polynomial $g = b_0 + b_1 t + \cdots + b_n t^n \in M[t]$, and so $[K(b_0, \ldots, b_n, \alpha) : K(b_0, \ldots, b_n)] < \infty$. Since $M : K$ is an algebraic extension, we know that $[K(b_0, \ldots, b_n) : K] < \infty$. Thus by the Tower Law we have

$$[K(b_0, \ldots, b_n, \alpha) : K(\alpha)][K(\alpha) : K] = [K(b_0, \ldots, d_n, \alpha) : K(b_0, \ldots, b_n)][K(b_0, \ldots, b_n) : K] < \infty.$$

Thus α is algebriac over K; this holds for all $\alpha \in L$, so $L : K$ is an algebraic extension.

The proof of the next lemma is a generalisation of the construction we employed to show that with K a field and irreducible $f \in K[t]$, there is a field extension L of K containing a root of [the homomorphic image of] f: We set $L = K[t]/I$ where I is the ideal in $K[t]$ generated by f. Since f is irreducible in $K[t]$, L is a field. We define a homomorphic embedding of $\varphi : K \to L$ by $\varphi(c) = c + I$, and we extend this to an embedding $\varphi : K[t] \to L[y]$ by mapping t to y. Then with $\alpha = t + I \in L$, we see that α is a root of $\varphi(f)$.

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 $u_j \in R$. Let $F : K$ be a field extension (relative to some homomorphism φ) so that F has a root β_j of each q_j, $j \in \mathcal{J}$. Extend φ to a homomorphism $\omega : R \to F$ by

$$\omega(t_i) = \begin{cases} \beta_i & \text{if } i \in \mathcal{J}, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\begin{aligned} 1 = \omega(1) &= \omega\left(\sum_{j \in \mathcal{J}} u_j q_j(t_j)\right) \\ &= \sum_{j \in \mathcal{J}} \omega(u_j) q_j(\beta_j) = 0, \end{aligned}$$

a contradiction. Thus $1 \notin A$, and $A \neq R$.

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 $\psi(c) = c + B$. We extend ψ to a map from $K[t]$ into $E[y]$ by $\psi(t) = y$. Take $i \in \mathcal{I}$, and write $q_i = a_0 + a_1 t + \cdots + a_m t^m$ $(a_0, \ldots, a_m \in K)$, and let $\alpha_i = t_i + B$; then

$$\psi(q_i) = (a_0 + B) + (a_1 + B)y + \cdots + (a_m + B)y^m$$

so

$$\psi(q_i)(\alpha_i) = (a_0 + a_1 t_i + \cdots + a_m t_i^m) + B = q_i(t_i) + B = 0 + B,$$

the zero element of E. Thus E contains a root of $\psi(q_i)$ for each irreducible $q_i \in K[t]$.

To see that $E : K$ is an algebraic extension, first let us ease notation by setting $K' = \psi(K)$. Then we see that $E = K'(\{\alpha_i\}_{i \in \mathcal{I}})$. Each α_i is algebraic over K', so each α_i is algebraic over K. Consequently E is algebraic over 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. □

Full disclosure: actually, we really have

$$E_0 = K \xrightarrow{\varphi_0} E_1 \xrightarrow{\varphi_1} E_2 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{n-1}} E_n \xrightarrow{\varphi_n} \cdots$$

where φ_n is a homomorphism extending φ_{n-1} $(n \in \mathbb{Z}_+)$. For consideration: how do we modify the above argument to be thoroughly honest?

Corollary 4.4. *Let K be a field. Then $\overline{K}$ is a maximal algebraic extension of K, meaning that if $L : \overline{K}$ is an algebraic extension, then $L \simeq \overline{K}$.*

Proof. Let $\overline{K}$ be an algebraic closure (which exists by Theorem 4.3), and suppose $L : \overline{K}$ be an algebraic extension relative to a homomorphism $\psi : \overline{K} \to L$ (so $\psi(\overline{K}) \subseteq L$). Take $\alpha \in L$. Since L is algebraic over $\overline{K}$, we have that $m_\alpha(\overline{K})$ exists and $m_\alpha(\overline{K}) = \psi(f)$ for some monic, irreducible $f \in \overline{K}[t]$. By Lemma 4.1, $\deg f = 1$, so $f = t - \alpha'$ for some $\alpha' \in \overline{K}$. Also, as α is a root of $\psi(f) = t - \psi(\alpha')$, we must have $\alpha = \psi(\alpha')$. Hence $L \subseteq \psi(\overline{K})$, and thus we get $L = \psi(\overline{K})$. From this we have $L \simeq \overline{K}$. □

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 $\alpha \in E \smallsetminus M$. 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 $M = \psi(L)$. □

Proposition 4.9. *Suppose $L : K$ is an algebraic extension, $\overline{L}$ is an algebraic closure of L, and $\overline{K}$ is an algebraic closure of K. Then $\overline{L} \simeq \overline{K}$.*

Proof. We know that $\overline{L}$ is an algebraic extension of L and L is an algebraic extension of K, so we know (by Proposition 1.15) that $\overline{L}$ is an algebraic extension of K. Also, $\overline{L}$ is algebraically closed, so $\overline{L}$ is an algebraic closure of K. □

Remark. Suppose $L : K$ is an algebraic extension. Then by Propositions 4.7 and 4.8, we have $\overline{L} \simeq \overline{K}$. Further, 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 $f \in K[t] \setminus K$. 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

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 $\lambda \in K$ 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 $S \subseteq K[t] \smallsetminus K$, 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 $f \in K[t] \smallsetminus K$, 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 $S \subseteq K[t] \setminus K$, 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 $f \in K[t] \smallsetminus K$. More generally, an extension $L : K$ is normal extension if and only if it is a splitting field extension for some $S \subseteq K[t] \smallsetminus K$. Equivalently, an extension $L : K$ is a normal extension if and only is it is an algebraic extension and for every $\alpha \in L$, $m_\alpha(K)$ splits over L.*

Proof. First suppose that $L : K$ is a normal extension. Thus $L : K$ is algebraic, so we can assume $K \subseteq L \subseteq \overline{K}$ where $\overline{K}$ is a fixed algebraic closure of K. Since this means that $L : K$ is an algebraic extension, for any $\alpha \in L$, $m_\alpha(K)$ exists. Set $S = \{m_\alpha(K) : \ \alpha \in L \}$; so $S \subseteq K[t] \smallsetminus K$. Also, each $m_\alpha(K)$ splits over L since $m_\alpha(K)$ is a irreducible element of $K[t]$ with a root (namely α) in L. Now suppose M is a field with $K : M : L$ so that every element of S splits over M. Thus for every $\alpha \in L$, $m_\alpha(K)$ splits over M, and so in particular, $\alpha \in M$. Hence $L \subseteq M$, so $M = L$. This means that $L : K$ is a splitting field extension for S.

Now suppose that $L : K$ is a splitting field extension for some $S \subseteq K[t] \smallsetminus K$. By Proposition 5.3, $L : K$ is an algebraic extension, so we can assume $K \subseteq L \subseteq \overline{K}$. We know $L = (R)$ where

$$R = \{\alpha \in \overline{K} : \text{ for some } f \in S, \ f(\alpha) = 0 \ \}.$$

Suppose that $g \in K[t]$ is irreducible over K, and $\gamma \in L$ is a root of g. Take $\delta \in \overline{K}$ so that δ is also a root of g. Thus for some $\lambda \in K^\times$, we have $m_\gamma(K) = \lambda g = m_\delta(K)$. So by Theorem 3.2, we can extend the identity map on K to an isomorphism $\sigma : K(\gamma) \to K(\delta)$ with $\sigma(\gamma) = \delta$. Then since $L : K$ is algebraic, by Theorem 4.5, we can extend σ to a homomorphism $\tau : L \to \overline{K}$. We have $\tau(L) = \tau(K)(\tau(R)) = K(\tau(R))$, and as we have seen before, since τ is a K-homomorphism and R is the set of (all) roots of elements of S, τ permutes the elements of R. Thus $\tau(R) = R$ and so $\tau(L) = K(\tau(R)) = K(R) = L$. In particular, this means that $\delta = \sigma(\gamma) = \tau(\gamma) \in L$. Hence for any irreducible $g \in K[t]$ with a root $\gamma \in L$, g splits over L, meaning that $L : K$ is a normal extension.

The last statement of the theorem is left as an exercise. □

Note: the above argument shows that $L : K$ is a normal extension if and only if $L : K$ is an algebraic extension and a splitting field extension for $\{m_\alpha(K) : \ \alpha \in L \}$. (Recall that with $L : K$ a normal extension, $L : K$ must be an algebraic extension and hence $m_\alpha(K)$ exists for each $\alpha \in L$.) Thus

we can also say that $L : K$ is a normal extension if and only if $L : K$ is an algebraic extension and for every $\alpha \in L$, $m_\alpha(K)$ splits over L.

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

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

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

To show (i) imples (iii): Suppose that (i) holds, and that $\sigma : L \to L$ is a K-automorphism. Take $\alpha \in M$. Since $M : K$ is assumed to be a normal extension, we know that $m_\alpha(K)$ splits over M, and σ must take α to a root of $m_\alpha(K)$ [this follows from Theorem 3.2]. Hence $\sigma(\alpha) \in M$. This argument holds for every $\alpha \in M$, so $\sigma(M) \subseteq M$.

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

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 M. Thus for λ the leading coefficient of g, we have $g = \lambda m_\alpha(K)$. Take $\beta \in \overline{K}$ a root of g. Thus $m_\beta(K) = \lambda^{-1} g = m_\alpha(K)$. Hence by Theorem 3.2, there is a K-isomorphism $\varphi : K(\alpha) \to K(\beta)$ so that $\varphi(\alpha) = \beta$. By Theorem 4.5, we can extend φ to a homomorphism $\psi : M \to \overline{K}$, and we can extend ψ to a homomorphism $\sigma : L \to \overline{K}$. Then by Proposition 6.1, $\tau(L) = L$. Hence $\psi(M) = \tau(M) \subseteq L$, and since we have assumed (ii), we have $\psi(M) = M$. Thus $\beta = \varphi(\alpha) = \psi(\alpha) \in M$. As this holds for any root $\beta \in \overline{K}$ of g, we have that g splits over M. As this holds for any irreducible $g \in K[t]$ that has a root in M, we have that $M : K$ is a normal extension. □

Definition. (nonexaminable:) 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. (nonexaminable:) *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 $K \subseteq L \subseteq \overline{K}$. Let

$$S = \{ m_\alpha(K) : \ \alpha \in L \},$$

and take $M \subseteq \overline{K}$ so that $M : K$ is a splitting field extension for S. Thus $M : K$ is a normal extension. Also, $L \subseteq M$ as for each $\alpha \in L$, α is a root of $m_\alpha(K) \in S$. Hence $M : K$ is a normal closure of $L : K$.

Now suppose $L : K$ 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 take $M \subseteq \overline{K}$ so that $M : K$ is a splitting field extension for f. Then one checks that $M : K$ is a normal closure for $L : K$. □

Remark. (nonexaminable:) 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 $L : K$.

As an exercise, one proves the following.

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

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

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 $g \in K[t] \setminus K$ [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 $g \in K[t] \setminus K$, and $E : K$ is a splitting field extension for some $h \in K[t] \setminus K$. 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. Suppose K is a field with $K \subseteq \overline{K}$ (where $\overline{K}$ is an algebraic closure of K). We say an irreducible polynomial $f \in K[t]$ is separable over K if has no repeated (equivalently, no multiple) roots in $\overline{K}$, meaning that $f = \lambda \prod_{i=1}^{d}(t - \alpha_i)$ where $\alpha_1, \ldots, \alpha_d \in \overline{K}$ are distinct. We say a polynomial $f \in K[t] \setminus K$ 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 over K. We say an algebraic extension $L : K$ is a separable extension if every $\alpha \in L$ is separable over K. (Note that if $L : M : K$ is a tower of fields and $L : K$ 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 will see that if $\mathrm{char} K = 0$, or if $\mathrm{char} K = p \neq 0$ and K is algebraic over its prime subfield, then every polynomial $f \in K[t] \setminus K$ is separable over K. So to construct an example of a polynomial that is not separable, we need to begin with a field that has nonzero characteristic and is transcendental over its prime subfield.) Fix a prime p and let F be field of order p. Set $K = F(y)$ where y is an indeterminate (and hence transcendental over K). Let $\overline{K}$ be an algebraic closure of K and assume that $K \subseteq \overline{K}$. Note that in $F[y]$, y is irreducible, and hence the polynomial $t^p - y$ is irreducible over $F[y]$ by Eisenstein's Criterion. Hence by Gauss' Lemma, $t^p - y$ is irreducible over K. Let $\alpha \in \overline{K}$ be a root of $t^p - y$; then

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

Hence $t^p - y$ is not separable over K.

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 $f \in K[t] \setminus K$ so that f is separable over K. If $g \in M[t] \setminus M$ 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 $L : M$. □

From Corollary 4.6, we have the following.

Proposition 7.2. *Suppose $L : M$ is an algebraic field extension. Say alpha $\in L$ and $\sigma : M \to \overline{M}$ is a homomorphism (where $\overline{M}$ is an algebraic closure of M). The number of distinct roots of $m_\alpha(M)$ in $\overline{M}$ is equal to the number of distinct roots of $\sigma(m_\alpha(M))$ in $\overline{M}$. Thus $m_\alpha(M)$ is separable over M if and only if $\sigma(m_\alpha(M))$ is separable over $\sigma(M)$.*

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 $K_i = K_{i-1}(\alpha_i)$. If each α_i is separable over K_{i-1} $(1 \leq i \leq n)$ then there are $[L : K]$ K-homomorphisms $\tau : L \to \overline{K}$; if, for some i $(1 \leq i \leq n)$, α_i is not separable over K_{i-1}, then there are fewer than $[L : K]$ K-homomorphisms $\tau : L \to \overline{K}$.*

Proof. Set $K_0 = K$, and for $i = 1, \ldots, n$, set $_i = K_{i-1}(\alpha_i)$. Let $\sigma_0 : K \to \overline{K}$ be the inclusion map.

Suppose $\tau : L \to \overline{K}$ is a K-homomorphism. 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. *Let K be a field.*

(a) *Suppose that $f \in K[t] \smallsetminus K$ 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.*
(b) *More generally, suppose $L : K$ is a splitting field extension for $S \subseteq K[t] \smallsetminus K$. 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 prove (a) and leave the proof of (b) as an exercise.

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. □

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 $K \subseteq E \subseteq L$, $K \subseteq F \subseteq L$ 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

$$D(fg) = (Df)g + f(Dg) \text{ and for } m \in \mathbb{Z}_+,\ D(f^m) = m(Df)f^{m-1}.$$

As an exercise, one proves the following.

Proposition 8.1. *Take $f \in K[t] \smallsetminus K$, and let $L : K$ be a field extension so that f splits over L. Assume that $K \subseteq L$. The following are equivalent:*

(i) *The polynomial f has a repeated in L.*
(ii) *There is some $\alpha \in L$ so that $f(\alpha) = 0 = (Df)(\alpha)$.*
(iii) *There is some irreducible $g \in K[t]$ so that 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 $\mathrm{char}K = p > 0$, 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. Let $\overline{K}$ be an algebraic closure of K, and identify K with its isomorphic image in $\overline{K}$ to assume $K \subseteq \overline{K}$.

Suppose first that f is inseparable over K; write

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

where $a_0, \ldots, a_n \in K$. By Proposition 8.1, there is an irreducible $g \in K[t]$ so that $g|f$ and $g|Df$. We know that either $Df = 0$ or $\deg Df < \deg f$; as f and g are irreducible over K, we must have $Df = 0$ and $g = \lambda f$ for some $\lambda \in K^\times$. Hence $f \in K[t^p]$ where $p = \mathrm{char}K > 0$.

Now suppose that $\mathrm{char}K = p > 0$ and $f \in K[t^p]$. Then $Df = 0$, and and so for any $\alpha \in \overline{K}$ so that $f(\alpha) = 0$, we also have $(Df)(\alpha) = 0$. Hence by Proposition 8.1, f has a repeated root. As f is irreducible over K, this means f is inseparable over K. □

Corollary 8.3. *Suppose that $\mathrm{char}K = 0$. Then all polynomials in $K[t] \smallsetminus$ 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 $charK = p > 0$, 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 K is a field with $charK = p > 0$, and suppose K is algebraic over its prime subfield. Then the Frobenius map ϕ on K is an automorphism of K.*

Corollary 8.6. *Suppose K is a field with $charK = p > 0$, and suppose K is algebraic over its prime subfield. Then all polynomials in $K[t] \setminus K$ 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 in $K[t]$. Thus $f = f_1^{m_1} \cdots f_r^{m_r}$ where $f_1, \ldots, f_r$ are distinct irreducible polynomials over K and $m_1, \ldots, m_r \in \mathbb{Z}_+$.

Case 1. Suppose 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 $\lambda_1 h_1 + \lambda_2 h_2 = 1$. As an exercise, one uses this to show that for some $c_0, \ldots, c_j, d_0, \ldots, d_k \in K$ where $j, k \in \mathbb{Z}_+$ and $c_j, d_k \neq 0$,

$$h_1 = c_0 + c_1 t^p + \cdots + c_j t^{jp},\ h_2 = d_0 + d_1 t^p + \cdots + d_k t^{kp}.$$

Then $g = (c_0 + c_1 t + \cdots + c_j t^j)(d_0 + d_1 t + \cdots + d_k t^k)$, meaning that g is reducible in $K[t]$.

Case 2. Suppose that $r = 1$; set $m = m_1$. So $f = f_1^m$ and $m > 1$ since by assumption, f is reducible in $K[t]$. As an exercise, one shows that if $p|m$ then all the coefficients of f are pth powers in K. Also as an exercise, one shows that if $p \nmid m$ then $g = g_1^m$ for some $g_1 \in K[t] \setminus K$. □

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). Then $L : K$ is a simple extension.*

Proof. Assume $K \subseteq L \subseteq \overline{K}$ 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 $r = [K(\alpha_1, \alpha_2) : K]$ (note that $r > 1$ as $\alpha_2 \notin K$). 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 $\delta \in K^\times$ 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 $n \in \mathbb{Z}_+$ so 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

Definitions. Let L be a field. For G a subgroup of $Aut(L)$, we define the fixed field of G to be

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

We say a field extension $L : K$ is a Galois extension if it is an extension that is normal and separable.

When $L : K$ is a finite Galois extension, the Fundamental Theorem of Galois Theory gives us a correspondence between fields M so that $L : M : K$ is a tower of field extensions, and subgroups of $Gal(L : K)$. To prepare for this we have the following, which one proves as an exercise.

Proposition 10.1. *Let L be a field. With M, M' subfields of L and H, H' subgroups of $Aut(L)$, we have the following.*

(a) *If $M' \subseteq M$ then $Gal(L : M') \supseteq Gal(L : M)$.*
(b) *If $H' \subseteq H$ then $Fix_L(H') \supseteq Fix_L(H)$.*
(c) *We have $M \subseteq Fix_L(Gal(L : M))$.*
(d) *We have $H \subseteq Gal(L : Fix_L(H))$.*
(e) *We have $Gal(L : M) = Gal(L : Fix_L(Gal(L : M)))$.*
(f) *We have $Fix_L(H) = Fix_L(Gal(L : Fix_L(H)))$.*

Theorem 10.2. *Suppose that L is a field and G is a subgroup of $Aut(L)$; let $K = Fix_L(G)$.*

(i) *Every G-orbit in L is finite if and only if $L : K$ is a Galois extension.*
(ii) *If $|G| < \infty$ then $L : K$ is a Galois extension, $G = Gal(L : K)$ and $|G| = [L : K]$.*

Proof. (i) Suppose that every G-orbit in L is finite, and take $\alpha \in L$. Let $\alpha, \alpha_2, \ldots, \alpha_r$ be the distinct elements in the G-orbit of α, and set

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

Take $\sigma \in G$. As $\sigma G = G$ [here the group operation in G is composition], the G-orbit of α is fixed by σ, and since σ is injective, σ permutes $\alpha, \alpha_2, \ldots, \alpha_r$. Hence f_α is fixed by σ, and this holds for each $\sigma \in G$; thus $f_\alpha \in K[t]$. This shows that α is algebraic over K, and $m_\alpha(K) | f_\alpha$. [In fact, as an exercise one can show that $f_\alpha = m_\alpha(K)$.] As f_α is constructed with no repeated roots, $m_\alpha(K)$ is separable over K, and $m_\alpha(K)$ splits over L. This holds for all $\alpha \in L$, so $L : K$ is a Galois extension.

Now suppose that $L : K$ is a Galois extension. Take $\alpha \in L$; thus α is algebraic over K and $m_\alpha(K)$ exists. Take $\sigma \in G$. As $K = Fix_L(G)$, we know that $\sigma(\alpha)$ is a root of $m_\alpha(K)$. Since $m_\alpha(K)$ has finitely many roots, this means that the G-orbit of α is finite; this holds for all $\alpha \in L$, completing the proof of (i).

(ii) Now say $|G| = n < \infty$. Thus for any $\alpha \in L$, the G-orbit has at most n elements. So by (i), $L : K$ is a Galois extension and for any $\alpha \in L$, $\deg m_\alpha(K) \leq n$. Then by Corollary 9.2, $[L : K] \leq n$. On the other hand, by Theorem 10.1(d), we have $G \subseteq Gal(L : K)$, and by Theorem 3.5, we have $|Gal(L : K)| \leq [L : K]$. Therefore we get

$$n = |G| \leq |Gal(L : K)| \leq [L : K] \leq n,$$

and thus [remembering that $G \subseteq Gal(L:K)$] $G = Gal(L:K)$. □

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 $K \subseteq L \subseteq \overline{K}$. Set $G = Gal(L:K)$.

To show (i) implies (ii): Suppose $L : K$ is Galois. Then by Proposition 6.2, $L : K$ is a splitting field extension for some $S \subseteq K[t] \setminus K$. Since $L : K$ is Galois and hence a separable extension, by Corollary 7.6, each $f \in S$ 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. So by the definition of G, $K \subseteq Fix_L(G)$. We now show that $Fix_L(G) \subseteq K$. For this, take $\alpha \in Fix_L(G)$. Let $\beta \in \overline{K}$ be a root of $m_\alpha(K)$. By Theorem 3.2, there is a K-homomorphism $\sigma : K(\alpha) \to \overline{K}$ with $\sigma(\alpha) = \beta$, and by Theorem 4.5, we can extend σ to a K-homomorphism $\tau : L \to \overline{K}$. By Propostion 6.1, we have $\tau(L) = L$. Therefore $\tau \in G$, and since $\alpha \in Fix_L(G)$, we have $\alpha = \tau(\alpha) = \sigma(\alpha) = \beta$. Hence α is the only root of $m_\alpha(K)$. Since every element of S is separable over K, Theorem 7.4 we know that $m_\alpha(K)$ is separable over K; thus $m_\alpha(K) = t - \alpha$, which means that $\alpha \in K$. This holds for all $\alpha \in Fix_L(G)$, so $Fix_L(G) \subseteq K$. Consequently $Fix_L(G) = K$.

To show (iii) implies (i): Suppose $K = Fix_L(G)$. Take $\alpha \in L$. We know $m_\alpha(K)$ exists, and for any $\sigma \in Gal(L:K)$, $\sigma(\alpha)$ is a root of $m_\alpha(K)$ lying in L. As $m_\alpha(K)$ has finitely many roots in L, this shows that each G-orbit in L is finite, so by Theorem 10.2, $L : K$ is a Galois extension. □

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 $L : K$ is a Galis extension; set $G = Gal(L:K)$. By Theorem 10.3, $K = Fix_L(G)$. By Theorem 3.5, $|G| \leq [L:K]$ and by assumption $[L:K] < \infty$, so by Theorem 10.2(ii), we have $|G| = [L:K]$.

Now say $|G| = [L:K]$. Thus there are at least $[L:K]$ K-homomorphisms $\sigma : L \to \overline{K}$, so by Corollary 7.5, $L : K$ is a separable extension. Then by Theorem 9.1, $L = K(\gamma)$ for some $\gamma \in L$, and $[L:K] = \deg m_\gamma(K)$. Since $L : K$ is separable, $m_\gamma(K)$ has $\deg m_\gamma(K)$ roots in $\overline{K}$. By Theorem 3.2, we have a one-to-one correspondence between the number of K-homomorphisms taking $K(\gamma)$ into L and the number of roots of $m_\gamma(L)$ that lie in L. Since each element of $Gal(L:K)$ are completely determined by its action on γ, and each element of $Gal(L:K)$ takes γ to a root of $m_\gamma(K)$, there are (at least) $|Gal(L:K)|$ roots of $m_\alpha(K)$ in L. AS $|Gal(L:K)| = [L:K]$ and $m_\gamma(K)$ has $[L:K]$ distinct roots in $\overline{K}$, all the roots of $m_\gamma(K)$ lie in L. Hence $m_\gamma(K)$ splits over L, and thus $L : K$ is a Galois extension. □

The next result will be useful in our computations when we apply the Fundamental Theorem of Galois Theory.

Corollary 10.5. *Suppose $L : K$ is a finite Galois extension with $K \subseteq L$ and $G = Gal(L : K)$. Let H be a subgroup of G and set $M = Fix_L(H)$. Then $L : M$ is a Galois extension with $H = Gal(L : M)$ and $[M : K] = [G : H]$.*

Proof. We have H a subgroup of $G = Gal(L : K)$, which is a finite group since $|G| = [L : K] < \infty$. By Theorem 10.2(ii), this means that $L : M$ is a Galois extension, $H = Gal(L : M)$, and $|H| = [L : M]$. By Theorem 10.4 we know $|G| = [L : K]$, so using the Tower Law we have

$$[G : H] = |G|/|H| = [L : K]/[L : M] = [M : K].$$

□

11. The Fundamental Theorem of Galois Theory and applications

Local notation. Fix a field L. For G a subgroup of $Aut(L)$, let $\phi(G)$ denote $Fix_L(G)$. For M a subfield of L, let $\gamma(M)$ denote $Gal(L : M)$.

In this notation, Proposition 10.1 says the following. With M, M' subfields of L and H, H' subgroups of $Aut(L)$, we have

(a) If $M' \subseteq M$ then $\gamma(M') \supseteq \gamma(M)$.
(b) If $H' \subseteq H$ then $\phi(H') \supseteq \phi(H)$.
(c) We have $M \subseteq \phi\gamma(M)$.
(d) We have $H \subseteq \gamma\phi(H)$.
(e) We have $\gamma(M) = \gamma\phi\gamma(M)$.
(f) We have $\phi(H) = \phi\gamma\phi(H)$.

Now we can finally state and prove Galois' main results.

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 extension $L : K_0$ is a Galois extension with $G = Gal(L : K_0)$ and $|G| = [L : K_0]$. Further, $K \subseteq K_0$, and if $L : K$ is a Galois extension then $K = K_0$.*
(b) *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.*
(c) *Suppose H is a subgroup of G. Then $H \lhd G$ if and only if $\phi(H) : K_0$ is a normal extension.*
(d) *When $H \lhd G$, we have $Gal(\phi(H) : K_0) \simeq G/H$. In particular, if $\sigma \in G$, we have $\sigma|_{\phi(H)} \in Gal(\phi(H) : K_0)$ 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) We know that $|Gal(L : K)| \leq [L : K]$ and by assumption, $[L : K] < \infty$. Thus Theorem 10.2(ii) tells us that $L : K_0$ is a Galois extension with $G = Gal(L : K_0)$ and $|G| = [L : K_0]$. By the definition of $Gal(L : K)$ and K_0, we have $K \subseteq K_0$. Theorem 10.3 tells us that $L : K$ is a Galois extension if and only if $K = K_0$.

(b) Suppose first that H is a subgroup of G (which we've seen is finite); so H is a finite subgroup of $Aut(L)$. Then by Theorem 10.2, $L : \phi(H)$ is a Galois extension and $H = Gal(L : \phi(H)) = \gamma\phi(H)$.

Now suppose M is a field with $K_0 \subseteq M \subseteq L$. Since $K \subseteq K_0$, we know by the Tower Law that

$$[L : M][M : K_0][K_0 : K] = [L : K] < \infty$$

and so $L : M$ is a finite extension. Since $L : K_0$ is a Galois extension, we know $L : M$ is a Galois extension (why?). Thus by theorem 10.3,

$$M = Fix_L(Gal(L : M)) = \phi\gamma(M).$$

Therefore ϕ and γ are inverses of each other.

(c) 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 (b),

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

Thus Theorem 6.4 implies that $\phi(H) : K_0$ is normal, as desired.

Now suppose that $\phi(H) : K_0$ is a normal extension. Take $\sigma \in G$ and $\tau \in H$. [We want to show that $\sigma^{-1}\tau\sigma \in H$.] We know by (b) that

$$H = \gamma\phi(H) = Gal(L : \phi(H)),$$

so for any $\beta \in \phi(H)$, we have $\tau(\beta) = \beta$. Take $\alpha \in \phi(H)$. As σ is a K_0-homomorphism, $\sigma(\alpha)$ is a root of $m_\alpha(K_0)$. Thus as $\phi(H) : K_0$ is a normal extension, we know $\sigma(\alpha)$. Therefore $\tau(\sigma(\alpha)) = \sigma(\alpha)$, and hence $\sigma^{-1}\tau\sigma(\alpha) = \alpha$. This holds for all $\alpha \in \phi(H)$, so $\sigma^{-1}\tau\sigma \in Gal(L : \phi(H) = \gamma\phi(H) = H$. As this holds for all $\sigma \in G$ and $\tau \in H$, we have $H \lhd G$.

(d) Suppose $H \lhd G$. (So $\phi(H) : K_0$ is a Galois extension.) Take $\sigma \in G = Gal(L : K_0)$. Let $\varphi = \sigma|_{\phi(H)}$. Thus $\varphi : \phi(H) \to L$. For any $\alpha \in \phi(H)$ we know $\varphi(\alpha)$ is a root of $m_\alpha(K_0)$ and hence $\varphi(\alpha) \in \phi(H)$ and $\phi(H) : K_0$ is a normal extension. So $\varphi : \phi(H) \to \phi(H)$ and as φ is a K_0-homomorphism and $\phi(H) : K_0$ is algebraic, $\varphi \in Aut(\phi(H))$. Thus $\sigma_{\phi(H)} = \varphi \in Gal(\phi(H) : K)$. For all $\sigma, \tau \in G$, we have $(\sigma\tau)|_{\phi(H)} = \sigma|_{\phi(H)}\tau|_{\phi(H)}$ so $\sigma \mapsto \sigma|_{\phi(H)}$ is a group homomorphism from G into $Gal(\phi(H) : K_0)$. Further, for any $\varphi \in Gal(\phi(H) : K_0)$, since $L : \phi(H)$ is an algebraic extension, φ can be extended to a homomorphism $\tau : L \to \overline{K}$, and since $L : \phi(H)$ is a normal extension, $\tau(L) = L$. Hence $\tau \in Gal(L : K_0)$, and thus the map $\sigma \mapsto \sigma|_{\phi(H)}$ is surjective. Also, σ is in the kernel of this map if and only if σ is the identity map on $\phi(H)$, meaning $\sigma \in Gal(L : \phi(H)) = \gamma\phi(H) = H$. So by one of the isomorphism theorems, $Gal(\phi(H) : K_0) \simeq G/H$. □

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'.) If $[L : \mathbb{Q}] = 8$ then $m_{\xi'}(\mathbb{Q}(\xi)) = (t - \xi')(t + \xi') = t^2 - 1 + i \in$

$\mathbb{Q}(\xi)[t]$, and we can construct all the elements of G by first construting a $\mathbb{Q}$-homomorphism ρ from $\mathbb{Q}(\xi)$ into L, and then extending this to an automorphism of L by mapping ξ' to a root of $\rho(t^2 - 1 + i) = t^2 - 1 + \rho(i)$.

So we consider the possibile elements of G, 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: (i) either σ_3 or σ_4 is in G; (ii) either σ_5 or σ_6 is in G; and (iii) either σ_7 or σ_8 is in G. Similarly, since ξ' is a root of f, we know: (iv) either σ_2 or σ_4 is in G; (v) either σ_5 or σ_7 is in G; and (vi) either σ_6 or σ_8 is in G.

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:

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

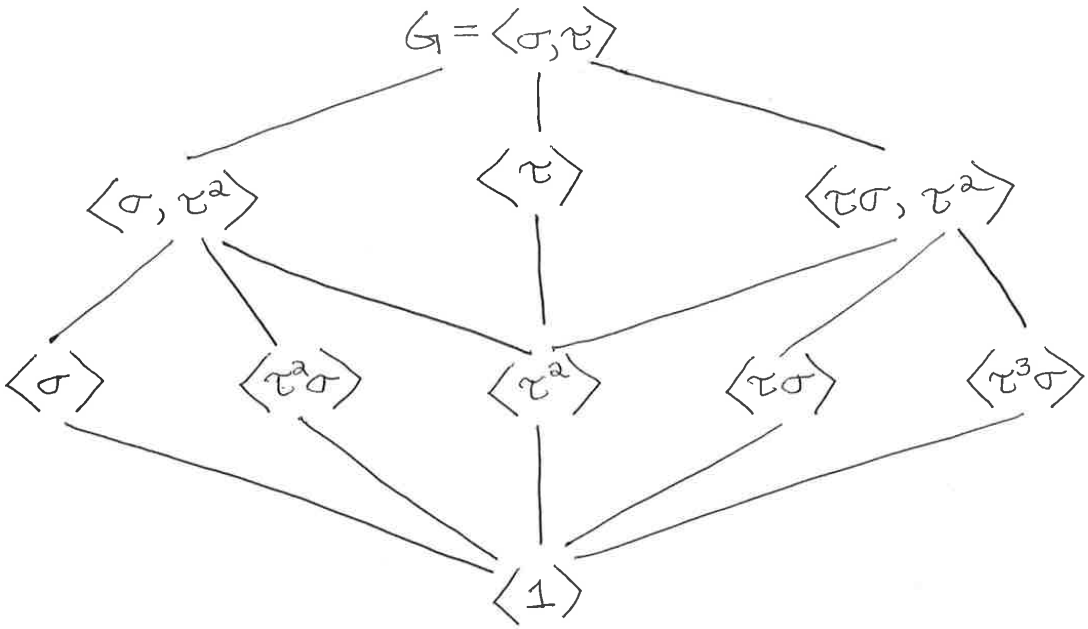
We know that $\tau\sigma$ fixes $\sqrt{2}$. Checking, we see that $\tau\sigma$ fixes $\xi+\xi'$, so we must have $m_\xi(E) = f_2$ [recall that $m_\xi(E)$ is unique]. Also note that $(\xi+\xi')^2 = 2+2\sqrt{2}$, so $\sqrt{2} \in \mathbb{Q}(\xi+\xi')$ and hence $f_2 \in \mathbb{Q}(\xi+\xi')[t]$. Thus $m_\xi(\mathbb{Q}(\xi+\xi'))$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



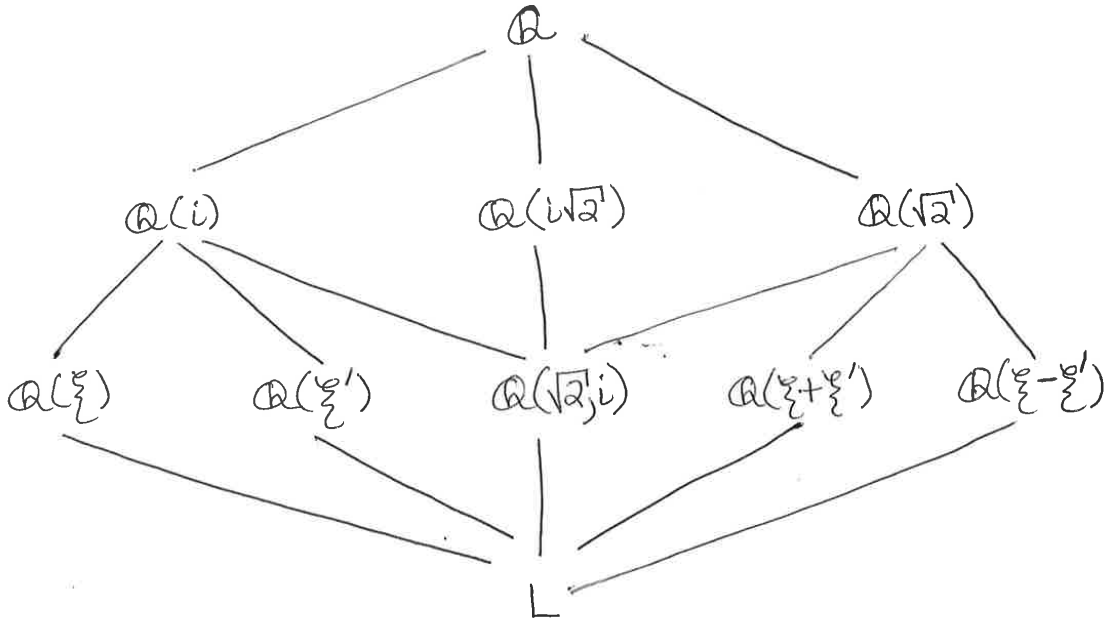


Diagram of the subgroups of $G = Gal(L:\mathbb{Q})$ and the corresponding fixed fields where $L:\mathbb{Q}$ is a splitting field extension for $f = t^4 - 2t^2 + 2$ and $\xi = \sqrt{1+i}$, $\xi' = \sqrt{1-i}$.

We now record another theorem about a compositum.

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, and by Corollary 10.5, the extension $E : E \cap F$ is Galois. Take $\sigma \in Gal(EF : F)$. Then $\sigma|_E$ is a homomorphism from E into EF that leaves $E \cap F$ pointwise fixed (meaning it is an $E \cap F$-homomorphism). Also, since $E : E \cap F$ is Galois and hence normal, by Theorem 6.4, $\sigma|_E \in Aut(E)$. Thus $\sigma|_E \in Gal(E : E \cap F)$. Thus defining $\psi(\sigma) = \sigma|_E$, we have that ψ is a map from $Gal(EF : F)$ to $Gal(E : E \cap F)$. One checks that ψ is in fact a homomorphism. Now take $\sigma \in \ker \phi$. Thus σ is the identity map on E; as $\sigma \in Gal(EF : F)$, σ is also the identity map on F, and hence σ is the identity map on EF. This means that ψ is injective. Take $H = \psi(Gal(EF : F))$, a subgroup of $Gal(E : E \cap F)$. Then by Theorem 10.3,

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

So by Corollary 10.5, $H = Gal(E : E \cap F)$. Therefore ψ is an isomorphism from $Gal(EF : F)$ onto $Gal(E : E \cap F)$.

(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. Using the Tower Law and (a), we have

$$[EF : E \cap F] = [EF : F][F : E \cap F] = [E : E \cap F][F : E \cap F].$$

Hence

$$\begin{aligned} |Gal(EF : E \cap F)| &= |Gal(E : E \cap F)| \cdot |Gal(F : E \cap F) \\ &= |Gal(E : E \cap F) \times Gal(F : E \cap F)|. \end{aligned}$$

As these quantities are finite and ω is injective, this shows that ω is bijective, proving (b). $\square$

Application: a proof of the Fundamental Theorem of Arithmetic – non-examinable.

Here we prove that any $f \in \mathbb{C}[t] \setminus \mathbb{C}$ splits over $\mathbb{C}$. For this, we need the following results from group theory.

Lemma 11.3. *Let G be a finite group (written multiplicatively). For $x \in G$, we let $C_x = \{gxg^{-1} : g \in G\}$ (the orbit of x under conjugation by G), and let $S_G(x) = \{g \in G : gxg^{-1} = x\}$ (the stabaliser, or centraliser, of x). Then $S_G(x)$ is a subgroup of G and $[G : S_G(x)] = |C_x|$.*

Proof. (Sketch) Tke $x \in G$. It is straightforward to verifythat $S_G(x)$ is subgroup of G. It is also straightforward to verify that there is a one-to-one correspondence between elements of C_x and cosets in the quotient $G/S_G(x)$. Hence $|C_x| = |G/S_G(x)| = [G : S_G(x)]$. □

Proposition 11.4. *Let G be a finite group and let $Z(G)$ be the cente of G (so $Z(G) = \{g \in G : \forall y \in G,\ yg = gy\}$). Suppose that G is not abelian. Let $x_1, \ldots, x_d \in G$ represent the distinct conjugacy classes C_x with more than one element. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{d} |C_{x_i}|.$$

Also, if $|G| = p^m$ with p prime and $m \in \mathbb{Z}_+$, then $|Z(G)|$ is a positive power of p.

Proof. Since G is not abelian, we know that $Z(G) \neq G$.

The group G acts on itself by conjugation, and hence G is partitioned into orbits (which with this group action are conjugacy classes). A conjugacy class C_x has only one element if and only if $x \in Z(G)$. Thus with $x_1, \ldots, x_d$ chosen as above, we have

$$|G| = |Z(G)| + \sum_{i=1}^{d} |C_{x_i}|.$$

Now suppose that $|G| = p^m$ with p prime and $m \in \mathbb{Z}_+$. For $x \in G$ we know by the above lemma that $|C_x| = [G : S_G(x)]$ and $S_G(x)$ is a subgroup of G. We know that $S_G(x) = G$ if and only if $x \in Z(G)$. Hence for $i = 1, \ldots, d$, we have that $|C_{x_i}| = [G : S_G(x_i)]$ is a positive power of p. Hence p divides $\sum_{i=1}^{d} |C_{x_i}|$, and since p divides $G|$, we must have that p divides $|Z(G)|$. Finally, since $Z(G)$ is a subgroup of G and $|G| = p^m$, we must have that $|Z(G)|$ is a positive power of p. □

Theorem 11.5. *Suppose G is a group with $|G| = p^m$ where p is prime and $m \in \mathbb{Z}_+$. Then G has a subgroup H of order p^{m-1}.*

Remark: When you prove the Sylow Theorems, you prove a stronger result, namely that a finite group with order divisible by p^k, p prime, the group has a subgroup of order p^k.

Proof. We argue by induction on m. When $m = 1$ we take $H = \{e\}$ where e denotes the identity element of G. Now suppose that $m \geq 1$ and that any group of order p^m has a subgroup of order p^{m-1}. Suppose that G is a group

of order p^{m+1}. We know from the preceding proposition that $|Z(G)| = p^k$ for some $k \in \mathbb{Z}_+$. Thus we can choose $a \in Z(G)$ so that $a \neq e$. Thus $\text{ord}(a) = p^r$ for some $r \in \mathbb{Z}_+$; set $y = a^{p^{r-1}}$; so $\text{ord}(y) = p$. Since $a \in Z(G)$ and hence $y \in Z(G)$, we know that $\langle y \rangle$ is a normal subgroup of G, and so $G' = G/\langle y \rangle$ is a group of order p^m. Hence by the induction hypothesis, G' has a subgroup H' of order p^{m-1}. By the Isomorphism Theorems, we know that G has a subgroup H containing $\langle y \rangle$ with $H' = H/\langle y \rangle$. Hence $p^{m-1} = |H'| = |H/\langle y \rangle| = |H|/p$ and so H is a subgroup of G with order p^m.

The theorem now follows by induction. □

Theorem 11.6. *Suppose that $f \in \mathbb{R}[t] \smallsetminus \mathbb{R}$. Then f splits over $\mathbb{C}$.*

Proof. Let $L : \mathbb{C}$ be a splitting field extension for f and identify $\mathbb{C}$ with its isomorphic image in L (so $\mathbb{R} \subseteq \mathbb{C} \subseteq L$). Thus $L : \mathbb{R}$ is a splitting field extension for $f \cdot (t^2 + 1)$ (check!). Let $G = Gal(L : \mathbb{R})$. As $\text{char}\mathbb{R} = 0$ and $L : \mathbb{R}$ is a splitting field extension for f, $L : \mathbb{R}$ is a finite Galois extension and so $|G| = [L : \mathbb{R}] = [L : \mathbb{C}][\mathbb{C} : \mathbb{R}] = [L : \mathbb{C}] \cdot 2$. This means that G has a Sylow 2-subgroup H, and with $d = [G : H]$, we know that d is odd. Set $M = Fix_L(H)$; so $[M : \mathbb{R}] = [G : H] = d$. By the Primitive Element Theorem, there is some $\gamma \in M$ so that $M = \mathbb{R}(\gamma)$, and then $d = [M : \mathbb{R}] = \deg m_\gamma(\mathbb{R})$. By Calculus, we know every odd degree polynomial over $\mathbb{R}$ has a root in $\mathbb{R}$, so this means that for some $\beta \in \mathbb{R}$, in $\mathbb{R}[t]$ we have $(t - \beta)|m_\gamma(\mathbb{R})$. Since $m_\gamma(\mathbb{R})$ is monic and irreducible over $\mathbb{R}$, we must have $t - \beta = m_\gamma(\mathbb{R})$; since γ is a root of $m_\gamma(\mathbb{R})$ we must have $\gamma = \beta \in \mathbb{R}$. Thus $d = 1$ and $|G| = 2^m$ for some $m \in \mathbb{Z}_+$.

Now let $G' = Gal(L : \mathbb{C})$. Note that as $L : \mathbb{R}$ is a Galois extension, so is $L : \mathbb{C}$. Thus

$$|G'| = [L : \mathbb{C}] = [L : \mathbb{R}]/[\mathbb{C} : \mathbb{R}] = 2^m/2 = 2^{m-1}.$$

For the sake of contradiction, suppose that $m > 1$. Then G' has a subgroup H' with $[G' : H'] = 2$ (why?). Let $M' = Fix_L(H')$, and take $\gamma' \in M'$ so that $M' = \mathbb{C}(\gamma')$. Hence $2 = [G' : H'] = [M' : \mathbb{C}] = \deg m_{\gamma'}(\mathbb{C})$. But by using the quadratic formula, any degree 2 polynomial over $\mathbb{C}$ splits over $\mathbb{C}$, contradicting that $m_{\gamma'}(\mathbb{C})$ is irreducible over $\mathbb{C}$ with degree 2. So we must have $m = 1$, meaning that $1 = |G'| = [L : \mathbb{C}]$ and hence $L = \mathbb{C}$. As f splits over L, we know that f splits over $\mathbb{C}$. □

Corollary 11.7. *For any $g \in \mathbb{C}[t] \smallsetminus \mathbb{C}$, g splits over $\mathbb{C}$.*

Proof. With $\overline{g}$ the complex conjugate of g, set $f = g\overline{g}$. Then $f = \overline{f} \in \mathbb{C}[t]$, meaning that $f \in \mathbb{R}[t]$. Also, $f \notin \mathbb{R}$, so by the above theorem, f splits over $\mathbb{C}$. As any root of g is a root of f, this means that g splits over $\mathbb{C}$. □

12. Finite fields

Throughout this section, L is a finite field. Recall that this means $\mathrm{char} L = p$ where p is a prime, and $|L| = p^n$ for some $n \in \mathbb{Z}_+$. Also, L contains a subfield F isomorphic to $\mathbb{Z}/p\mathbb{Z}$, called the prime subfield of L; as we saw in Theorem 8.4, $F = \{\alpha \in L : \ \phi(\alpha) = \alpha \}$ where ϕ denotes the Frobenius map (so $\phi(\alpha) = \alpha^p$). As L is a finite field, $[L : F] < \infty$ and $p^n = |L| = p^{[L:F]}$; hence $[L : F] = n$. This means that $L : F$ is an algebraic extension, so by Corollary 8.6, $L : F$ is a separable extension. We also know that as a multiplicative group, $L^\times$ 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. Let $L : \mathbb{Z}/p\mathbb{Z}$ be a splitting field extension for $f = t^q - t$, and let K be the isomorphic image of $\mathbb{Z}/p\mathbb{Z}$ in L. Note that as $|K^\times| = p - 1$, for any $\alpha \in K$ we have $\alpha^p = \phi(\alpha) = \alpha$, and thus K is the prime subfield of L. Also note that $Df = qt^{q-1} - 1 = -1$ (where D is the derivative operator), and so by Proposition 8.1, f has no repeated roots. Let R the set of roots of f in L; we easily see that $K \subseteq R$. We claim that R is a ring. To see this, take $\alpha, \beta \in R$; then $f(\alpha + \beta) = f(\alpha) + f(\beta) = 0$, $f(-\alpha) = -f(\alpha) = 0$, and $f(\alpha\beta) = \alpha^q(\beta^q - \beta) + \beta(\alpha^q - \alpha) = 0$. Thus R is a ring. Further, as L is a field and hence contains no zero divisors, R is a finite integral domain, so (by an exercise in Algebra 2) R is a field. [Recall: for $\alpha \in R$, $\alpha \neq 0$, $\{\alpha\gamma : \ \gamma \in R \}$ is a subset of R with $|R|$ elements, and hence for some $\gamma \in R$, $\alpha\gamma = 1$.] Thus R is a subfield of L with q elements, $K \subseteq R$, and f splits over R. As $L : K$ is a splitting field extension for f, we must have $R = L$ and hence $|L| = q = p^n$.

Suppose M is another field of order q; let E denote the prime subfield of M. Hence $E \simeq \mathbb{Z}/p\mathbb{Z}$, and $M : \mathbb{Z}/p\mathbb{Z}$ is a splitting field extension for f. Thus 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 M that is a splitting field for $t^q - t$, and hence $M \simeq \mathbb{F}_q$. □

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 its Galois group generated by the Frobenius map and $Gal(\mathbb{F}_q : \mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$, and with the Frobenius map as a generator of $Gal(\mathbb{F}_q : \mathbb{F}_p)$.*
(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

Before we define the meaning of radicals, we first make the following observation. Take $f \in K[t] \smallsetminus K$; assume $K \subseteq \overline{K}$. Let $\alpha_1, \ldots, \alpha_n \in \overline{K}$ be the distinct roots of f. Thus with $L = K(\alpha_1, \ldots, \alpha_n)$, $L : K$ is a splitting field extension for f. Take $\sigma \in Gal(L : K)$. As σ is a K-homomorphism, σ is completely determined by its action on $\alpha_1, \ldots, \alpha_n$. We know from Proposition 3.1 and the fact that σ is injective that $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\} = \{\alpha_1, \ldots, \alpha_n\}$; in other words, σ permutes $\alpha_1, \ldots, \alpha_n$. Also, as σ is a K-homomorphism, σ is completely determined by its action on $\alpha_1, \ldots, \alpha_n$. Hence we can identify σ with an element of S_n, the symmetric group on n "letters" (which we can take to be $\alpha_1, \ldots, \alpha_n$, or the subscripts of these elements of $\overline{K}$). In this way we can identify $Gal(L : K)$ with a subset G' of S_n, and G' is necessarily a group as multiplication of elements in G' corresponds to composition of elements in $Gal(L : K)$.

Definitions. Suppose that $L : K$ is a field extension, and $\beta \in L$; assume $K \subseteq L$. 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} $(1 \leq i \leq r)$. We say $f \in K[t] \smallsetminus K$ is solvable by radicals if there is a radical extension of K over which f splits.

We know that when K is a field with characteristic different from 2, 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 $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. 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 $\alpha_2 = -b/a - \alpha_1$).

Now we consider cubic and quartic polynomials. We first introduce the discriminant of a polynomial, which detects whether a polynomial has repeated roots.

Let K be a field, and assume that $K \subseteq \overline{K}$ (where $\overline{K}$ is an algebraic closure of K). Take $f \in K[t]$ with $\deg f \leq 2$. In $\overline{K}[t]$, $f = a\prod_{i=1}^{n}(t - \alpha_i)$ for some $\alpha_1, \ldots, \alpha_n \in \overline{K}$ and $a \in K^\times$. 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; note that $D(f)$ is independent of the ordering of the roots of f, so it is well-defined. (Also note that when $f = at^2 + bt + c$ with $a \neq 0$ and $\mathrm{char}K \neq 2$, we have $D(f) = b^2 - 4ac$.) 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 $\alpha_1, \ldots, \alpha_n$.

With $K, f, \alpha_1, \ldots, \alpha_n$ be as above, let $L = K(\alpha_1, \ldots, \alpha_n)$, and take

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

a square root of $D(f)$. We know from the discussion at the beginning of this section that $Gal(L : K)$ is isomorphic to some subgroup G' of S_n. Take $\sigma \in Gal(L : K)$ and let φ_σ be the element of S_n corresponding to σ. If φ_σ is a transposition $(k\ m)$ with $1 \le k < m \le n$, then

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

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

Theorem 13.1. *Suppose that $f \in K[t]$ is irreducible and separable 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, $Gal(L : K) \simeq S_3$.*

Proof. Assume $K \subseteq L \subseteq \overline{K}$. With $a \in K^\times$ the lead coefficient of f, we have

$$f = a(t - \alpha_1)(t - \alpha_2)(t - \alpha_3)$$

for some $\alpha_1, \alpha_2, \alpha_3 \in \overline{K}$, and $L = K(\alpha_1, \alpha_2, \alpha_3)$. We know that

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

As discussed above, $Gal(L : K) \simeq G'$ for some subgroup G' of S_3. Hence $|Gal(L : K)|$ divides 6. Also,

$$3 = [K(\alpha_1) : K] = [L : K]/[L : K(\alpha_1)],$$

so 3 divides $[L : K]$. 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. Thus $\sigma(d) = d$ for all $\sigma \in Gal(L : K)$ if and only if $Gal(L : K) \simeq A_3$. When $Gal(L : K) \simeq A_3$, d is fixed by $Gal(L : K)$, so $\pm d \in K$ (and hence D has a square root in K). When $Gal(L : K) \simeq S_3$, d is not fixed by $Gal(L : K)$, so $\pm d \notin K$. □

Now suppose $\mathrm{char} K \ne 2$, and $f = t^4 + a_3t^3 + a_2t^2 + a_1t + a_0$ is separable and irreducible in $K[t]$. Let $L : K$ be a splitting field extension for f; assume $K \subseteq L \subseteq \overline{K}$. To classify $Gal(L : K)$, we introduce an auxiliary polynomial r, the "resolvant", which is a degree 3 polynomial in $K[t]$. With $F : K$ a splitting field extension for r (with $K \subseteq F \subseteq \overline{K}$), we will find that $F \subseteq L$, and the structure of $Gal(L : K)$ is determined by $[F : K]$ (and, in the case that $[F : K] = 2$, whether f is irreducible over F.)

Set

$$g(t) = f(t - a_3/4) = t^4 + b_2t^2 + b_1t + b_0$$

for some $b_2, b_1, b_0 \in K$. Let $\alpha_1, \ldots, \alpha_4 \in \overline{K}$ denote the roots of g. Thus $b_0 = \alpha_1\alpha_2\alpha_3\alpha_4$, $b_1 = -\sum_{i<j<k} \alpha_i\alpha_j\alpha_k$, $b_2 = \sum_{i<j} \alpha_i\alpha_j$ and $0 = \sum_i \alpha_i$. Set

$L = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. As the roots of f are $\beta_i = \alpha_i + \frac{a_3}{4}$, $L : K$ is a splitting field extension for g and for f. By Corollary 7.6, $L : K$ is separable and hence g is also separable over K. (Thus $D(g) \neq 0$.)

Now we define the resolvant r by

$$r = (t-u)(t-v)(t-w)$$

where

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

With $F = K(u, v, w)$, $F : K$ is a splitting field extension for r. An easy verification shows

$$u-v = (\alpha_1-\alpha_4)(\alpha_3-\alpha_2),\ u-w = (\alpha_1-\alpha_3)(\alpha_4-\alpha_2),\ v-w = (\alpha_1-\alpha_2)(\alpha_4-\alpha_3),$$

we find that $D(r) = D(g)$. Thus $D(r) \neq 0$, which means that u, v, w are distinct. Hence at least two of the values u, v, w are non-zero, so by rearranging $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ if necessary, we can assume that u, v are non-zero.

Now set

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

Thus $K(u', v', w') \subseteq K(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = L$. Remembering $\sum_i \alpha_i = 0$, we have

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

Thus we have $L = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \subseteq K(u', v', w')$, so $K(u', v', w') = L$. Also,

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

since $\sum_i \alpha_i = 0$. As $u'v'w' = -b_1 \in K$ and u', v' are non-zero, we have $-\dfrac{u'v'}{b_1} = w'$ and $-\dfrac{(u'v')^2}{b_1^2} = w$, so

$$K(u', v', w') = K(u', v') \text{ and } F = K(u, v, w) = K(u, v).$$

Theorem 13.2. *Suppose that charK $\neq 2$, and that $f \in K[t]$ is separable, monic, 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) *We have $[L : K] \geq 4$, $[L : K]$ divides 24, $[L : F]$ divides 4, and $[F : K]$ 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* $Gal(L : K) \simeq C_4$ *(a cyclic group of order 4).*
(e) *If* $[F : K] = 1$ *then* $Gal(L : K) \simeq V_4$*.*

(Recall that

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

the dihedral group of order 8, and

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

the Klein-4 group.)

Proof. (a) We know $[L : K] \geq 4$ as f is irreducible over K with $\deg f = 4$. Also, $Gal(L : K)$ is isomorphic to a subgroup of S_4, so $|Gal(L : K)| = [L : K]$ divides 24. Similarly, as $F : K$ is a splitting field extension for a degree 3 polynomial with distinct roots, $Gal(F : K)$ is isomorphic to a subgroup of S_3, and hence $|Gal(F : K)| = [F : K]$ divides 6. Also, $[K(u', v) : K(u, v)] \leq 2$ (as $(u')^2 = -u$), and $[K(u', v') : K(u', v)] \leq 2$ (as $(v')^2 = -v$). Hence by the Tower Law, $[L : F] = [K(u', v') : F] = 1, 2$ or 4.

To prove the other statements, we first interpret the action of $\tau \in Gal(L : K)$ on $\{u, v, w\}$ using elements of S_4. First let $\{i, j, k, \ell\} = \{1, 2, 3, 4\}$, and consider $\varphi = (i \ k)$; so $\varphi(i \ j)(k \ \ell)\varphi = (i \ \ell)(j \ k)$ and

$$(\alpha_{\varphi(i)} + \alpha_{\varphi(j)})(\alpha_{\varphi(k)} + \alpha_{\varphi(\ell)}) = (\alpha_k + \alpha_j)(\alpha_i + \alpha_\ell).$$

More generally (recalling that any element of S_4 is a product of transpositions), for $\varphi \in S_4$ and $\varphi^{-1}(i \ j)(k \ \ell)\varphi = (i' \ j')(k' \ \ell')$, we find that

$$(\alpha_{\varphi(i)} + \alpha_{\varphi(j)})(\alpha_{\varphi(k)} + \alpha_{\varphi(\ell)}) = (\alpha_{i'} + \alpha_{j'})(\alpha_{k'} + \alpha_{\ell'}).$$

Thus, identifying u with $(1\ 2)(3\ 4)$, v with $(1\ 3)(2\ 4)$, and w with $(1\ 4)(2\ 3)$, for any $\tau \in Gal(L : K)$ and $\varphi = \varphi_\tau$ (the element of S_4 corresponding to τ), we find that $\tau(u)$ corresponds to $\varphi^{-1}(1\ 2)(3\ 4)\varphi$, $\tau(v)$ corresponds to $\varphi^{-1}(1\ 3)(2\ 4)\varphi$, and $\tau(w)$ corresponds to $\varphi^{-1}(1\ 4)(2\ 3)\varphi$.

Now set $V = \{(1), \ (1\ 2)(3\ 4), \ (1\ 3)(2\ 4), \ (1\ 4)(2\ 3)\}$. It is not hard to verify that V is a normal subgroup of S_4. Also, $(1\ 2)(3\ 4)$ has 3 conjugates in S_4 (being the non-identity elements of V), so by a theorem in group theory (see Corollary 3.1.3 of "Algebra" by Grillet), the centraliser N of $(1\ 2)(3\ 4)$ has $|S_4|/3 = 8$ elements. More precisely,

$$N = V \cup \{(1\ 2), \ (3\ 4), \ (1\ 3\ 2\ 4), \ (1\ 4\ 2\ 3)\} = \big\langle (1\ 3\ 2\ 4), \ (1\ 2) \big\rangle.$$

So N is one of the 3 Sylow 2-subgroup of S_4, and $N \simeq D_4$. The centraliser of $(1\ 3)(2\ 4)$ is $(1\ 4)N(1\ 4)$, and the centraliser of $(1\ 4)(2\ 3)$ is $(1\ 3)N(1\ 3)$ (the other 2 Sylow 2-subgroups of S_4). Further, $N \cap (1\ 4)N(1\ 4) \cap (1\ 3)N(1\ 3) = V$. So for $\tau \in Gal(L : K)$, τ fixes u, v, and w if and only if $\varphi_\tau \in V$. Hence with G the subgroup of S_4 corresponding to $Gal(L : K)$, the group $Gal(L : F)$ corresponds to $G \cap V$. As $F : K$ is a Galois extension, by Theorem 11.1 we have $Gal(F : k) \simeq G/(G \cap V)$.

Suppose $|G| = 24$; then $[F : K] = 6$ and $[L : F] = 4$.

Suppose $|G| = 12$. Then $G = A_4$, the only subgroup of S_4 of order 12. Hence $V \subseteq G$ and $[F : K] = |G/V| = 3$.

Suppose $|G| = 8$. Thus G is one of the 3 Sylow 2-subgroups, and $Gal(L : K) \simeq D_4$. Also, $V \subseteq G$ (as discussed above), so

$$[F : K] = |Gal(F : K)| = |G/V| = 2.$$

Further, as V is transitive on $\{1, 2, 3, 4\}$, $V \subseteq G$ and $Gal(L : F)$ corresponds to $V \cap G$, $Gal(L : F)$ is transitive on $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$. Hence $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are roots of $m_{\alpha_1}(F)$ (see Theorem 3.2). As $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are distinct, this means $4 \leq \deg m_{\alpha_1}(F)$, and as $m_{\alpha_1}(F) | m_{\alpha_1}(K)$ with $\deg m_{\alpha_1}(K) = \deg g = 4$, we have $\deg m_{\alpha_1}(F) = 4$. So g, and thus f, are irreducible over F. (Recall that the roots of f are $\alpha_i + \frac{a_3}{4}$, $1 \leq i \leq 4$, with $a_3 \in K$, so the same argument that shows g is irreducible over F shows f is irreducible over F.)

Suppose $|G| = 4$ and $V \subseteq G$; then $V = G$ and hence $[L : F] = |Gal(L : F)| = 4$, $[F : K] = |Gal(F : K)| = |G/V| = 1$, and $Gal(L : K) \simeq V_4$.

Suppose $|G| = 4$ and $V \not\subseteq G$. The only order 4 subgroups of S_4 that are transitive on $\{1, 2, 3, 4\}$ are V and order 4 cyclic groups. Thus $[L : F] = |Gal(L : F)| = |G \cap V| < 4$ and since $4 = |G| = [L : K] = [L : F][F : K]$, we have $[L : F] = 1$ or 2. As $[F : K] | 6$, we must have $[L : F] = 2 = [F : K]$, and hence f must be reducible over F.

There is one situation above where $[F : K] = 6$, and in this case $Gal(L : K) \simeq S_4$ (proving (b)). There is one situation where $[F : K] = 3$, and in this case $Gal(L : K) \simeq A_4$ (proving (c)). There are two situations where $[F : K] = 2$; when f is irreducible over F we have $Gal(L : K) \simeq D_4$, and when f is reducible over F we have $Gal(L : K) \simeq C_4$ (proving (d)). Finally, there is one situation where $[F : K] = 1$, in which case $Gal(L : K) \simeq V_4$ (proving (e)). $\square$

14. Cyclotomic polynomials and cyclotomic extensions

Definitions. Let K be a field. 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 $K^\times$.) 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 14.1. *For $n \in \mathbb{Z}_+$, the primitive nth roots of unity in $\mathbb{C}$ are $e^{2\pi i k/n}$ where $k \in \mathbb{Z}$ with $hcf(k, n) = 1$. Thus with $\zeta = e^{2\pi i/n}$,*

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

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 14.2. *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 14.3. *For $n \in \mathbb{Z}_+$, $\Phi_n \in \mathbb{Z}[t]$ and Φ_n is monic.*

Proof. (Here we outline the proof.) We argue by induction on n. We have $\Phi_1 = t - 1$, which is monic and in $\mathbb{Z}[t]$.

Now suppose that $n > 1$ and assume that for all $d \in \mathbb{Z}_+$ with $d < n$, Φ_d is monic and in $\mathbb{Z}[t]$. Thus

$$\prod_{\substack{d|n \\ d<n}} \Phi_d$$

is also monic and in $\mathbb{Z}[t]$. Then using polynomial division (which we leave to the reader), we find that

$$\Phi_n = (t^n - 1) / \prod_{\substack{d|n \\ d<n}} \Phi_d$$

is also monic and in $\mathbb{Z}[t]$. □

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*.)

Proposition 14.4. *For $n \in \mathbb{Z}_+$, Φ_n is irreducible over $\mathbb{Q}$.*

Proof. We know that $\Phi_1 = t - 1$ and $\Phi_2 = t + 1$ are irreducible over $\mathbb{Q}$, so suppose $n > 2$. For the sake of contradiction, suppose Φ_n is reducible over $\mathbb{Q}$. It follows from Gauss' Lemma that Φ_n is reducible over $\mathbb{Z}$. Thus $\Phi_n = qr$ for some $q, r \in \mathbb{Z}[t]$ with q irreducible in $\mathbb{Z}[t]$ and r not a unit in $\mathbb{Z}[t]$. As qr is monic, the lead coefficients of q and r are either both -1 or both 1; adjusting as necessary, we can assume q and r are both monic. (Note that by Gauss' Lemma, q is irreducible in $\mathbb{Q}[t]$ as well.)

Let $\varepsilon \in \mathbb{C}$ be a root of q and $\zeta \in \mathbb{C}$ be a root of r. This means ε, ζ are primitive nth roots of unity, so there is some $k \in \mathbb{Z}_+$ so that $\zeta = \varepsilon^k$. Note that $\gcd(k, n) = 1$ as ζ is a primitive nth root of 1. By Dirichlet's Theorem on primes in arithmetic progressions, there is a prime p so that $p \equiv k \pmod{n}$ and hence $p \nmid n$ and $\zeta = \varepsilon^p$. Thus ε is a root of $r(t^p)$. Since q must be $m_\varepsilon(\mathbb{Q})$, q divides $r(t^p)$ and so $r(t^p) = qs$ for some $s \in \mathbb{Q}[t]$; actually, since r, q and thus s are monic, polynomial division shows that $s \in \mathbb{Z}[t]$.

Now we consider our polynomials modulo p (where p is as above); for $f \in \mathbb{Z}[t]$, let $\overline{f}$ be the image of f in $(\mathbb{Z}/p\mathbb{Z})[t]$. We first observe that by Proposition 8.1, $\overline{t^n - 1}$ has no repeated roots in an algebraic closure of $\mathbb{Z}/p\mathbb{Z}$: we have $D(\overline{t^n - 1}) = \overline{nt^{n-1}}$ with $\overline{n} \neq \overline{0}$ and $n - 1 \geq 1$; so $\overline{0}$ is the only root of $D(\overline{t^n - 1})$, but $\overline{0}$ is not a root of $\overline{t^n - 1}$. Also note that $\deg \overline{q} = \deg q \geq 1$ (so $\overline{q}$ is not a unit). We have $(\overline{r}(t))^p = \overline{r}(t^p)$ (why?). So for some $s \in \mathbb{Z}[t]$, we have $\overline{r}(t^p) = \overline{qs}$ (why?). With $\overline{h}$ an irreducible factor of $\overline{q}$ in $(\mathbb{Z}/p\mathbb{Z})[t]$, we have $\overline{h} | \overline{r}$ with $\overline{r}$ denoting $\overline{r}(t)$ (why?). Hence $\overline{h}^2 | \overline{\Phi}_n$ (why?). Thus $\overline{h}^2$ divides $\overline{t^n - 1}$. However, this implies that $\overline{t^n - 1}$ has a repeated root, which is not the case.

Thus Φ_n must be irreducible over $\mathbb{Q}$. □

As an exercise, one proves the following.

Proposition 14.5. *Fix $n \in \mathbb{Z}$ with $n > 1$, and let ε be a primitive nth root of unity. Then $\mathbb{Q}(\varepsilon) : \mathbb{Q}$ is a Galois extension, and $Gal(\mathbb{Q}(\varepsilon) : \mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.*

The next proof also uses Dirichlet's Theorem on primes in arithmetic progressions.

Theorem 14.6. *Every finite abelian group is the Galois group of some Galois extension of $\mathbb{Q}$.*

Proof. Let G be a finite abelian group. From a theorem in group theory (see, for instance, Theorem 2.2.6 in "Algebra" by Grillet), $G \simeq C_1 \times \cdots \times C_k$ for some $k \in \mathbb{Z}_+$ where each C_i is a cyclic group of some order n_i. By Dirichlet's Theorem, there are distinct primes $p_1, \ldots, p_k$ so that for each subscript i, we have $p_i \equiv 1 \pmod{n_i}$. Set $n = p_1 \cdots p_k$, and let $\varepsilon = \mathrm{e}^{2\pi i/n} (\in \mathbb{C})$. Thus $\mathbb{Q}(\varepsilon) : \mathbb{Q}$ is a Galois extension, and from Proposition 14.5, $Gal(\mathbb{Q}(\varepsilon) : \mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Recall that for $r, s \in \mathbb{Z}_+$ with $\mathrm{hcf}(r, s) = 1$, we know by the Chinese Remainder Theorem that $\mathbb{Z}/rs\mathbb{Z} \simeq (\mathbb{Z}/r\mathbb{Z}) \times (\mathbb{Z}/s\mathbb{Z})$. (To see this, take $u, v \in \mathbb{Z}$ so that $ru + sv = 1$; define

$$\psi : (\mathbb{Z}/r\mathbb{Z}) \times (\mathbb{Z}/s\mathbb{Z}) \to \mathbb{Z}/rs\mathbb{Z}$$

by $\psi((a + r\mathbb{Z}, b + s\mathbb{Z})) = rub + sva + rs\mathbb{Z}$. One easily shows that ψ is a well-defined, injective homomorphism, and since

$$|(\mathbb{Z}/r\mathbb{Z}) \times (\mathbb{Z}/s\mathbb{Z})| = |\mathbb{Z}/rs\mathbb{Z}| = rs < \infty,$$

ψ is surjective.) Consequently $(\mathbb{Z}/rs\mathbb{Z})^{times} \simeq (\mathbb{Z}/r\mathbb{Z})^\times \times (\mathbb{Z}/s\mathbb{Z})^\times$. Thus induction gives us

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times.$$

For each i, $1 \leq i \leq k$, $(\mathbb{Z}/p_i\mathbb{Z})^\times$ is cyclic of order $p_i - 1$ (recall that the multiplicative group of a finite field is cyclic). Since $n_i | p_i - 1$, $(\mathbb{Z}/p_i\mathbb{Z})^\times$ contains a subgroup H_i with $|H_i| = (p_i - 1)/n_i$, and hence $(\mathbb{Z}/p_i\mathbb{Z})^\times / H_i$ is cyclic with order n_i. As

$$(\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times \simeq (\mathbb{Z}/n\mathbb{Z})^\times \simeq Gal(\mathbb{Q}(\varepsilon) : \mathbb{Q})$$

and $H_1 \times \cdots \times H_k$ is a normal subgroup of $(\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times$, $Gal(\mathbb{Q}(\varepsilon) : \mathbb{Q})$ contains a normal subgroup H with

$$H \simeq H_1 \times \cdots \times H_k.$$

With $M = Fix_{\mathbb{Q}(\varepsilon)}(H)$, by Theorem 11.1, $M : \mathbb{Q}$ is a Galois extension with

$$\begin{aligned} Gal(M : \mathbb{Q}) &\simeq G/H \\ &\simeq (\mathbb{Z}/p_1\mathbb{Z})^\times / H_1 \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times / H_k \\ &\simeq C_1 \times \cdots \times C_k \\ &\simeq G, \end{aligned}$$

proving the theorem. □

15. Cyclic extensions and Abel's Theorem

In this section we introduce the notion of a field extension being cyclic, and we prove some nice results, helping us review some of our previous results.

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

As a consequence of Propositions 8.1 and 14.2 we have the following.

Proposition 15.1. *Suppose K is a field, $\theta \in K^\times$, $n \in \mathbb{Z}$ with $n > 1$, and charK $\nmid n$. Let $L : K$ be a splitting field extension for $t^n - \theta$; assume $K \subseteq L \subseteq \overline{K}$.*

(a) *There is a primitive nth root of unity, ε, in L.*
(b) *The extension $L : K(\varepsilon)$ is a cyclic extension, and $|Gal(L : K(\varepsilon))|$ divides n.*
(c) *The polynomial $t^n - \theta$ is irreducible over $K(\varepsilon)$ if and only if $|Gal(L : K(\varepsilon))| = n$.*

Proof. (a) Since char$K \nmid n$, we know from Theorem 8.1 that $t^n - \theta$ has no repeated roots in L. Thus for $\alpha, \varepsilon \in \overline{K}$ so that α is a root of $t^n - \theta$ and ε is a primitive nth root of unitey, the roots of $t^n - \theta$ are $\alpha, \alpha\varepsilon, \ldots, \alpha\varepsilon^{n-1}$. Hence $\alpha, \alpha\varepsilon \in L$, and since $\alpha \neq 0$, we have $\varepsilon \in L$.

(b) Take $\sigma \in Gal(L : K(\varepsilon))$. Since $L = K(\alpha, \varepsilon)$, σ is determined by its action on α. Since $\sigma(\alpha)$ must be a root of $t^n - \theta$, we have $\sigma(\alpha) = \alpha\varepsilon^k$ for some $k \in \mathbb{Z}$, $0 \leq k < n$. Define $\psi : Gal(L : K(\varepsilon)) \to \mathbb{Z}/n\mathbb{Z}$ by $\psi(\sigma) = k + n\mathbb{Z}$ where $\sigma(\alpha) = \alpha\varepsilon^k$. One easily checks that ψ is a homomorphism [of groups]. Also,

$$\begin{aligned}\ker\psi &= \{\sigma \in Gal(L : K(\varepsilon)) : \ \psi(\sigma) = 0 + n\mathbb{Z} \ \} \\ &= \{\sigma \in Gal(L : K(\varepsilon)) : \ \sigma(\alpha) = \alpha \ \} \\ &= \{1_{K(\varepsilon)}\}.\end{aligned}$$

Thus ψ is injective, so $Gal(L : K(\varepsilon))$ is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$, which is necessarily cyclic (why?). Also, $|Gal(L : K(\varepsilon))|$ divides n (why?).

(c) With $\alpha \in L$ a root of $t^n - \theta$ (as above), we know $m_\alpha(K(\varepsilon))$ divides $t^n - \theta$. As

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

(why?), so $t^n - \theta$ is irreducible over $K(\varepsilon)$ if and only if $|Gal(L : K(\varepsilon))| = n$ (why?). □

From this, we deduce the following.

Theorem 15.2. *(Abel's Theorem) Suppose $q \in \mathbb{Z}_+$ is prime, charK $\neq q$, and $\theta \in K^\times$. Suppose $t^q - \theta$ is reducible over K. Then:*

(a) *the polynomial $t^q - \theta$ has a root in K;*
(b) *the polynomial $t^q - \theta$ splits over K if and only if K contains a primitive qth root of unity.*

Proof. Let $L : K$ be a splitting field extension for $t^q - \theta$, and assume $K \subseteq L$. Let $g \in K[t]$ be a factor of $t^q - \theta$ so that g is irreducible over K; we can assume g is monic (why?). Thus g is separable over K (why?) and g splits

over L (why?). With $\beta \in L$ a root of g, we know that β is a root of $t^q - \theta$ (why?). By Proposition 15.1, L contains a primitive qth root of unity, ε. So $\beta, \beta\varepsilon, \ldots, \beta\varepsilon^{q-1}$ are the q distinct roots of $t^q - \theta$ in L.

(a) Let $d = \deg g$. Thus in $L[t]$,

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

for some $m_2, \cdots, m_d \in \mathbb{Z}_+$ with $1 \leq < m_2 < \cdots < m_d < q$ (why?). Since $g \in K[t]$, with $m = m_2 + \cdots + m_d$ we have $\beta\varepsilon^m \in K$. We know $0 < d < q$ (why?), and since q is prime (and hence $\mathbb{Z}/q\mathbb{Z}$ is a field), there is some $d' \in \mathbb{Z}_+$ with $dd' = 1 + q\ell$ for some $\ell \in \mathbb{Z}_+$. Thus

$$(\beta^d\varepsilon^m)^{d'} = \beta^{1+q\ell}\varepsilon^{md'} = \beta\theta^\ell\varepsilon^{md'}$$

(why?). We have $\beta^d\varepsilon^m, \theta \in K$ with $\theta \neq 0$, so $\beta\varepsilon^{md'} \in K$ and $\beta\varepsilon^{md'}$ is a root of $t^q - \theta$, proving (a).

(b) With $\alpha = \beta\varepsilon^{md'}$, we know α is a root of $t^q - \theta$, so $\alpha, \alpha\varepsilon, \ldots, \alpha\varepsilon^{q-1}$ are the distinct roots of $t^q - \theta$ (why?). As $\alpha \in K$, we see that $t^q - \theta$ splits over K if and only if $\varepsilon \in K$ (which is equivalent to saying that $t^q - \theta$ splits over K if and only if K contains a primitive qth root of unity (why?)). □

Closing remarks. There are some topics in Galois Theory that are not covered in these notes, such as the relationship between solvable groups and polynomials that are solvable by radicals (see, for instance, section 7.10 in the book "Algebra" by Grillet). One can also study Galois extensions with infinite degree. Another direction of research involving Galois Theory is that of Galois representations; this is currently a very active area of research, often applied to the study of elliptic curves. Through the internet, you can find many references to Galois representations and elliptic curves, and there are quite a few textbooks presenting these topics.