MA4203 Galois Theory Notes

Thang Pang Ern

The reader is highly recommended to refer to the books by Gallian (solutions) and Cox (solutions) for further examples. Moreover, the reader should have a good foundation in MA2202 Algebra I and MA3201 Algebra II before reading this set of notes although we will recap these concepts along the way.

Reference books:

(1). Dummit, D. S. and Foote, R. M. (2003). *Abstract Algebra 3rd Edition*. Wiley.

(2). Gallian, J. (2009). *Contemporary Abstract Algebra 7th Edition*. Cengage Learning.

(3). Cox, D. (2010). *Galois Theory 2nd Edition*. Wiley.

Contents

Evariste Galois (1811-1832)

Ne pleure pas, Alfred!

1. Cubic Equations

1.1. *Cardano's Formulae*

Let x be a variable and $\mathbb{C}$ denote the set of complex numbers. Define $\mathbb{C}[x]$ to be the set of polynomials with complex coefficients, i.e.

$$\mathbb{C}[x] = \left\{a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n : a_n \neq 0, a_i \in \mathbb{C} \text{ for all } 0 \leq i \leq n\right\}.$$

Here, the degree of the polynomial is defined to be n. Note that the degree of the *constant polynomial* $p(x) = a_0$, where $a_0 \neq 0$, is 0, and the degree of $p(x) = 0$ is not defined. Moreover, recall that a polynomial of degree $n \geq 1$ is monic if $a_n = 1$. In general, we may replace $\mathbb{C}$ by a commutative ring R and define a polynomial of degree n over R, say $p(x) \in R[x]$, as an expression of the form

$$a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n \quad \text{where } a_i \in R \text{ for all } 0 \leq i \leq n \text{ and } a_n \neq 0.$$

Let $\alpha \in \mathbb{C}$. Then, α is a solution of the polynomial equation

$$a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

where $a_i \in \mathbb{C}$ for all $0 \leq i \leq n$ if

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0.$$

Since $\mathbb{C}$ is a field and $a_n \neq 0$, we may divide the polynomial equation by a_n and consider the polynomial equation where the polynomial is monic. The solutions to the polynomial equation are known as the roots or zeros of the polynomial.

One recalls from O-Level that the solution to the quadratic equation

$$x^2 + bx + c \quad \text{is} \quad \alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

This can be easily derived using a method known as 'completing the square'. The quantity nested within the square root, $b^2 - 4c$, is known as the discriminant of the polynomial $x^2 + bx + c$.

Suppose the two roots of the quadratic equation $x^2 + bx + c = 0$ are

$$\alpha = \frac{-b + \sqrt{b^2 - 4c}}{2} \quad \text{and} \quad \beta = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

Then, one verifies that $(\alpha - \beta)^2 = b^2 - 4c$, which implies that the discriminant of the quadratic polynomial can be viewed as the square of the difference between its two roots. From this perspective, it allows us to define the discriminant of polynomials of degrees greater than 2.

Definition 1.1 (discriminant). Let

$$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0.$$

The discriminant of $p(x)$, denoted by Δ, is defined to be

$$\Delta = \prod_{1 \le i < j \le n} \left(\alpha_i - \alpha_j\right)^2 \quad \text{where } \alpha_1, \ldots, \alpha_n \text{ are solutions to the equation } p(x) = 0.$$

This motivates our discussion of Cardano's formulae. Recall that a cubic monic polynomial equation is of the form

$$x^3 + bx^2 + cx + d = 0.$$

Using the substitution $x = y - b/3$, we obtain the following depressed cubic equation:

$$y^3 + py + q = 0 \quad \text{where} \quad p = -\frac{b^2}{3} \text{ and } q = \frac{2}{27}b^3 - \frac{bc}{3} + d.$$

Even if the coefficient of the x^3 term is not 1, we can always transform any cubic equation to a depressed cubic (will discuss this in due course). In order to find the solutions to a cubic polynomial equation, it suffices to find the solutions to the reduced cubic polynomial equation.

When $p = 0$, the equation $y^3 + py + q$ has obvious solutions

$$-q^{1/3}, -\omega q^{1/3}, -\omega^2 q^{1/3} \quad \text{where} \quad \omega = e^{2\pi i/3} \text{ is a cube root of unity.}$$

This is not that interesting, so we shall consider the case where $p \neq 0$. Let $y = u + v$, and observe that the depressed cubic now becomes

$$u^3 + v^3 + 3uv(u+v) + p(u+v) + q = 0.$$

We need to choose u and v aptly. In fact, the substitution $3uv = -p$ works. Noting that $p \neq 0$ (consequently $u \neq 0$), we see that

$$u^3 + v^3 + q = u^3 + \left(-\frac{p}{3u}\right)^3 + q = 0.$$

This yields

$$u^6 + qu^3 - \frac{p}{27} = 0 \quad \text{which implies} \quad u^3 = -\frac{q}{2} \pm \frac{\sqrt{q^2 + 4p^3/27}}{2}$$

We omit the remaining details of the derivation as they are trivial.

Theorem 1.1 (Cardano's formula). The solutions to the depressed cubic equation $y^3+py+q=0$ are

$$\begin{aligned} y_1 &= z_1+z_2 \\ y_2 &= \omega z_1+\omega^2 z_2 \\ y_3 &= \omega^2 z_1+\omega z_2 \end{aligned}$$

where

$$z_1 = \sqrt[3]{\frac{1}{2}\left(-q+\sqrt{q^2+\frac{4p^3}{27}}\right)} \quad \text{and} \quad z_2 = -\frac{p}{3z_1}$$

1.2. *Permutations of Roots*

In Cardano's formula (Theorem 1.1), we can express z_1 and z_2 in terms of y_1,y_2,y_3 and deduce the six solutions of $z^6+qz^3-p^3/27=0$ (recall we dealt with the polynomial equation $u^6+qu^3-p/27=0$ earlier). In particular, the six solutions are

$$\begin{aligned} z_1 &= \frac{1}{3}\left(y_1+\omega^2 y_2+\omega y_3\right) \\ z_2 &= \frac{1}{3}\left(y_1+\omega y_2+\omega^2 y_3\right) \\ \omega z_1 &= \frac{1}{3}\left(\omega y_1+y_2+\omega^2 y_3\right) \\ \omega z_2 &= \frac{1}{3}\left(\omega y_1+\omega^2 y_2+y_3\right) \\ \omega^2 z_1 &= \frac{1}{3}\left(\omega^2 y_1+\omega y_2+y_3\right) \\ \omega^2 z_2 &= \frac{1}{3}\left(\omega^2 y_1+y_2+\omega y_3\right) \end{aligned}$$

Recall from MA2202 that the symmetric group on 3 letters, S_3, can be interpreted as the set of bijections from $\{1,2,3\}$ to $\{1,2,3\}$. For any permutation $\sigma \in S_3$, we define

$$\sigma \circ y_j = y_{\sigma(j)}.$$

Observe that S_3 permutes the six roots of $z^6+qz^3-p^3/27$. For example, the permutation $\sigma=(1\,2\,3)$ leads to the following identities:

$$(1\,2\,3)\circ z_1 = \omega z_1 \quad (1\,2\,3)\circ \omega z_1 = \omega^2 z_1 \quad (1\,2\,3)\circ \omega^2 z_1 = z_1$$

To see why this makes sense, we only justify $(1\,2\,3)\circ z_1 = \omega z_1$. Since 1 is mapped to 2, then $\sigma\circ y_1 = y_2$; since 2 is mapped to 3 and 3 is mapped to 1, then $\sigma\circ y_2 = y_3$ and $\sigma\circ y_3 = y_1$.

As such, we see that $(1\,2\,3)\circ z_1^3 = z_1^3$, implying that it is the invariance of z_1^3, under the action of the permutation $(1\,2\,3)$, that allows us to determine the roots of the cubic polynomial.

Also, observe that

$$(1)(2\,3)\circ z_1 = (2\,3)\,z_1 = z_2.$$

Applying $(1\,2\,3)$ and $(1\,2\,3)(1\,2\,3)$ to z_2, we deduce that z_1 is sent to all the roots of the cubic polynomial $z^6+qz^3-p^3/27$ via the action of S_3.

1.3. *Cubic Equations over* $\mathbb{R}$

Recall that the discriminant of the depressed cubic y^3+py+q is

$$\Delta = (y_1-y_2)^2(y_1-y_3)^2(y_2-y_3)^2.$$

One notes that Δ can also be written as $\Delta = -4p^3-27q^2$. Now, we assume that $y^3+py+q=0$ has distinct roots y_1,y_2,y_3 so that Δ is a non-zero real number. There is a nice result on the roots of the cubic equation $y^3+py+q=0$ depending on the sign of Δ (Theorem 1.2).

Theorem 1.2. Suppose the cubic polynomial $y^3+py+q\in\mathbb{R}[y]$ has distinct roots and discriminant $\Delta\neq 0$. Then, the following hold:

(i) $\Delta>0$ if and only if the roots are all real

(ii) $\Delta<0$ if and only if the equation has only one real root and the other two roots are complex conjugates of each other

Example 1.1 (Cox p. 22 Question 9)**.** When divided by 4,

$$4t^3-3t-\cos 3\theta \quad \text{gives} \quad t^3-\frac{3}{4}t-\frac{1}{4}\cos 3\theta \text{ which is monic.}$$

Show that the discriminant of this polynomial is $\frac{27}{16}\sin^2 3\theta$.

Solution. Let $\alpha_1,\alpha_2,\alpha_3$ be the roots of the polynomial equation. By Vieta's formula,

$$\begin{aligned}\alpha_1+\alpha_2+\alpha_3 &= 0\\ \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 &= -\frac{3}{4}\\ \alpha_1\alpha_2\alpha_3 &= \frac{1}{4}\cos 3\theta\end{aligned}$$

The discriminant is

$$\Delta = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2$$

for which with some tedious algebraic manipulation, one can show that Δ is indeed the aforementioned value. □

Example 1.2 (Bombelli)**.** In 1550, Rafael Bombelli applied Cardano's formula to the cubic $y^3-15y-4=0$. This polynomial has discriminant $\Delta = 13068>0$, so all three roots are real. Bombelli noted that one root is $y=4$ and used Cardano's formula to deduce that

$$4=\sqrt[3]{2+11i}+\sqrt[3]{2-11i} \quad \text{for appropriate choices of cube roots.}$$

To understand this formula, Bombelli noted that $(2+i)^3=2+11i$ and $(2-i)^3=11-i$. Hence, the cube roots in the above formula are $2+i$ and $2-i$, for which their sum is 4.

From this perspective of Cardano's method, complex numbers are unavoidable when $\Delta>0$. However, is it possible that there are other ways of expressing the roots which only involve real radicals? For the case when the polynomial is an irreducible cubic with real roots, the answer is no. We will discuss this further when we introduce the Fundamental Theorem of Galois Theory.

François Viète developed a trigonometric approach to solve cubic equations, providing a way to obtain real solutions without resorting to complex numbers. Although Cardano's formulas often lead to complex values even for cubics with positive discriminants, Viète's method uses trigonometric functions instead of radicals to reveal purely real solutions. This approach, known as the trigonometric solution of the cubic, sidesteps complex numbers by leveraging trigonometric identities and transformations.

Our starting point is the trigonometric identity

$$\cos 3\theta=4\cos^3\theta-3\cos\theta \quad \text{which can be derived using the addition formula.}$$

If we write this as $4\cos^3\theta-3\cos\theta-\cos 3\theta=0$, then $t_1=\cos\theta$ is a root of the cubic equation $t^3-3t-\cos 3\theta=0$. However, replacing θ with $\alpha=\theta+2\pi/3$ gives the same cubic polynomial since $\cos 3\alpha=\cos 3\theta$. It follows that $t_2=\cos\alpha=\cos(\theta+2\pi/3)$ is another root of $4t^3-3t-\cos 3\theta=0$. Similarly, $t_3=\cos(\theta+4\pi/3)$ is also a root.

2. Symmetric Polynomials and Roots of Polynomials

2.1. *Symmetric Polynomials*

Definition 2.1. A polynomial in $x_1,\ldots,x_n$ with coefficients in F is a finite sum of terms, which are expressions of the form

$$cx_1^{k_1}\ldots x_n^{k_n} \quad \text{where } c\in F \text{ and } k_j\in\mathbb{Z}_{\geq 0}.$$

A term is non-zero if $c\neq 0$. The set of polynomials in n variables with coefficients in F is denoted by $F\left[x_1,\ldots,x_n\right]$.

Definition 2.2 (discriminant)**.** Given $n\geq 2$ variables $x_1,\ldots,x_n$ over a field F, the discriminant associated with $x_1,\ldots,x_n$ is defined to be

$$\Delta\left(x_1,\ldots,x_n\right)=\prod_{i<j}\left(x_i-x_j\right)^2\in F\left[x_1,\ldots,x_n\right].$$

Example 2.1. Adapted from page 51 Question 3 of Cox's textbook, we shall verify that the discriminant formula holds for a monic quadratic polynomial, i.e. consider $f=x^2+bx+c\in F[x]$. Then we shall justify that $\Delta(f)=b^2-4c$. To see why, let α and β denote the roots of f. Then, we have

$$\begin{aligned}\Delta(f)&=(\alpha-\beta)^2\\&=(\alpha+\beta)^2-4\alpha\beta\\&=b^2-4c\quad\text{by Vieta's formula}\end{aligned}$$

Definition 2.3 (degree)**.** We have the following:

$$\begin{aligned}&\text{the total degree of a non-zero term } cx_1^{k_1}\ldots x_n^{k_n} \quad\text{is}\quad k_1+\ldots+k_n\\&\text{the total degree of a polynomial } f=f\left(x_1,\ldots,x_n\right) \text{ in } n \text{ variables}\quad\text{is}\\&\text{the maximum of the total degree of the non-zero term of } f.\end{aligned}$$

The degree of the polynomial is denoted by $\deg(f)$.

Example 2.2. The discriminant of a polynomial in n variables, $\Delta\left(x_1,\ldots,x_n\right)$, is of degree $n(n-1)$.

Note that if

$$f\left(x_1,\ldots,x_n\right) \text{ and } g\left(x_1,\ldots,x_n\right) \quad \text{are non-zero polynomials,}$$

then

$$\deg(f)+\deg(g)=\deg(fg).$$

This shows that $F[x_1,\ldots,x_n]$ is an integral domain (recall from MA3201). In fact, a stronger claim is that $F[x_1,\ldots,x_n]$ is a unique factorisation domain (UFD). Recall from MA3201 that an integral domain R is a UFD if every non-zero element of R can be written in the form

$$up_1\ldots p_k \quad \text{where} \quad u \text{ is a unit and } p_i \text{ are irreducibles in } R.$$

Recall that S_n is a group under the composition of bijections. The group S_n acts on $F[x_1,\ldots,x_n]$ via the following way:

$$\sigma\cdot f(x_1,\ldots,x_n) = f\left(x_{\sigma(1)},\ldots,x_{\sigma(n)}\right) \quad \text{where} \quad \sigma\in S_n \text{ and } f(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n].$$

Definition 2.4 (symmetric polynomial)**.** A polynomial $f(x_1,\ldots,x_n)\in\mathbb{C}[x_1,\ldots,x_n]$ is symmetric if

$$\sigma\cdot f(x_1,\ldots,x_n) = f(x_1,\ldots,x_n) \quad \text{for any } \sigma\in S_n.$$

Example 2.3 (Δ is a symmetric polynomial)**.** Another representation of the discriminant is as follows:

$$\Delta(x_1,\ldots,x_n) = (-1)^{n(n-1)/2}\prod_{i\neq j}\left(x_i-x_j\right)$$

i.e. it can be shown that

$$\prod_{i<j}\left(x_i-x_j\right)^2 = (-1)^{n(n-1)/2}\prod_{i\neq j}\left(x_i-x_j\right).$$

Recall from MA2202 that for any permutation $\sigma\in S_n$, σ is a disjoint product of cycles, where each cycle can be written as a product of transpositions. In other words,

$$(a_1\,a_2\,\ldots\,a_{n-1}\,a_n) = (a_1\,a_n)\ldots(a_1\,a_3)(a_1\,a_2),$$

where the map is read from right to left. One can show that Δ is invariant under the action of 2-cycles, and consequently, Δ is a symmetric polynomial.

Definition 2.5 (elementary symmetric polynomials)**.** Given variables $x_1,\ldots,x_n$, define

$$\sigma_{n,j}(x_1,\ldots,x_n) = \sum_{1\leq m_1<\ldots<m_j\leq n} x_{m_1}\ldots x_{m_j} \quad \text{to be the elementary symmetric polynomials.}$$

This is the sum of all possible products of j distinct variables.

Example 2.4. We have

$$\sigma_{n,0}(x_1,\ldots,x_n) = 1 \quad \text{and} \quad \sigma_{n,1}(x_1,\ldots,x_n) = \sum_{i=1}^{n} x_i.$$

Moreover, $\sigma_{n,n}(x_1,\ldots,x_n) = x_1\ldots x_n$.

Theorem 2.1 is a key property of the elementary symmetric polynomials.

Theorem 2.1. Let $x_1,\ldots,x_n$ be variables over a field F. Then given another variable x, we have

$$(x-x_1)\ldots(x-x_n)=x^n-\sigma_{n,1}x^{n-1}+\ldots+(-1)^r\sigma_{n,r}x^{n-r}+\ldots+(-1)^n\sigma_{n,n}.$$

Here, $\sigma_{n,j}=\sigma_{n,j}(x_1,\ldots,x_n)$.

In fact, it is clear from Theorem 2.1 that $\sigma_{n,j}$ are symmetric polynomials.

The elementary symmetric polynomials serve as a basis for the set of symmetric polynomials. In fact, we have a precise statement for it.

Theorem 2.2. Any symmetric polynomial in $F[x_1,\ldots,x_n]$ can be uniquely written as a polynomial in $\sigma_{n,1},\ldots,\sigma_{n,n}$ with coefficients in F.

Example 2.5 (Cox p. 42 Question 18)**.** Suppose the complex numbers α,β,γ satisfy the equations

$$\begin{aligned}\alpha+\beta+\gamma&=3\\ \alpha^2+\beta^2+\gamma^2&=5\\ \alpha^3+\beta^3+\gamma^3&=12\end{aligned}$$

Prove that $\alpha^n+\beta^n+\gamma^n$ is always an integer for all $n\geq 4$. Also, evaluate $\alpha^4+\beta^4+\gamma^4$.

Solution. Consider the monic polynomial (leading coefficient 1) $p(x)=x^3+bx^2+cx+d$. Say that the roots of the equation $p(x)=0$ are α,β,γ. As such, by Vieta's formula, we have

$$\alpha+\beta+\gamma=-b \quad \text{so} \quad b=-3.$$

Squaring the first equation yields the identity

$$\begin{aligned}(\alpha+\beta+\gamma)^2&=\alpha^2+\beta^2+\gamma^2+2\alpha\beta+2\beta\gamma+2\gamma\alpha\\ 9&=5+2(\alpha\beta+\beta\gamma+\gamma\alpha)\\ \alpha\beta+\beta\gamma+\gamma\alpha&=2\end{aligned}$$

By Vieta's formula again, we have $\alpha\beta+\beta\gamma+\gamma\alpha=c$, so $c=2$. Lastly, cubing the first equation yields

$$\begin{aligned}(\alpha+\beta+\gamma)^3&=\alpha^3+\beta^3+\gamma^3+3\alpha^2\beta+3\alpha^2\gamma+3\beta^2\alpha+3\beta^2\gamma+3\gamma^2\alpha+3\gamma^2\beta+6\alpha\beta\gamma\\ 27&=12+3\alpha^2(\beta+\gamma)+3\beta^2(\gamma+\alpha)+3\gamma^2(\alpha+\beta)+6\alpha\beta\gamma\\ 5&=\alpha^2(3-\alpha)+\beta^2(3-\beta)+\gamma^2(3-\gamma)+2\alpha\beta\gamma\\ 5&=3\alpha^2-\alpha^3+3\beta^2-\beta^3+3\gamma^2-\gamma^3+2\alpha\beta\gamma\\ 5&=15-12+2\alpha\beta\gamma\\ \alpha\beta\gamma&=1\end{aligned}$$

By Vieta's formula one more time, we have $\alpha\beta\gamma = -d$, so $d = -1$. As such, α, β, γ are roots of the cubic equation $x^3 - 3x^2 + 2x - 1 = 0$. For $\alpha \geq 4$, we have $\alpha^n = 3\alpha^{n-1} - 2\alpha^{n-2} + \alpha^{n-3}$, which is merely a consequence of the factor theorem. We obtain similar equations for β and γ. Define s_n to be

$$s_n = \alpha^n + \beta^n + \gamma^n \quad \text{so} \quad s_n = 3s_{n-1} - 2s_{n-2} + s_{n-3}.$$

The rest follows by induction as we have $s_0 = 3$ and s_1, s_2, s_3 are integers as well. In particular, $s_4 = 35$. □

3. Extension Fields

3.1. *Elements of Extension Fields*

Recall from MA3201 that

$$\text{a field } F \quad \text{is} \quad \text{a ring such that every non-zero element has a multiplicative inverse.}$$

For any field F, observe that $n \cdot 1_F$ is the sum of n copies of 1_F, where 1_F is the identity element. We shall abbreviate the notation as $n1_F$. If $n1_F = 0$ and n is the smallest positive integer for which this happens, then n must be a prime. Suppose otherwise, then n can be written as $n = ab$, with either $a1_F = 0$ or $b1_F = 0$, contradicting the minimality of n (in fact, those who have picked up MA1100 can understand this too). As such,

$$p1_F = 0 \quad \text{for some prime } p.$$

When this happens, we say that the field F has characteristic p, and we write $\text{char}(F) = p$. If $n1_F \neq 0$ for all non-zero integers, then the field F has characteristic 0.

Example 3.1. The field of complex numbers $\mathbb{C}$ is of characteristic 0, so $\text{char}(\mathbb{C}) = 0$.

Example 3.2. For p prime, the field $\mathbb{Z}/p\mathbb{Z}$ is of characteristic p.

As such, given a field F, can we construct new fields that contain F (idea of field extension coming up). To answer this question, we recall the following construction from MA3201. In particular, $\mathbb{C}$ can be constructed from $\mathbb{R}[x]/\left(x^2+1\right)\mathbb{R}[x]$, where $\left(x^2+1\right)$ is the principal ideal generated by x^2+1.

We can construct more fields using a technique similar to constructing $\mathbb{C}$ from $\mathbb{R}[x]/\left(x^2+1\right)\mathbb{R}[x]$.

Definition 3.1 (prime subfield)**.** Let F be a field. The prime subfield of F is

$$\text{the subfield generated by } 1_F.$$

From Definition 3.1, we infer that if $\text{char}\, F = 0$, then its prime subfield is $\mathbb{Q}$. On the other hand, if $\text{char}\, F = p$, then the prime subfield is $\mathbb{F}_p$ which is the finite field of p elements.

Definition 3.2 (field extension)**.** Let

$$\varphi : F \to L \quad \text{be a ring homomorphism of fields.}$$

Then, L is a field extension of F via φ. We will usually identify F with its image $\varphi(F) = \{\varphi(a) : a \in F\} \subseteq L$ and write $F \subseteq L$. Moreover, the following are equivalent:

$$L \text{ is a field extension of } F \quad \text{and} \quad F \text{ is a subfield of } F$$

In Definition 3.2, we mentioned that for a field extension $F \subseteq L$ is such that F can be identified with its image $\varphi(F)$, where $\varphi : F \to L$ is a ring homomorphism. In fact, this idea consistently appears throughout Mathematics. For example, we can consider $\mathbb{Z} \subseteq \mathbb{Q}$. Since $\mathbb{Q}$ is the field of fractions of the integral domain $\mathbb{Z}$, then an element $a/b \in \mathbb{Q}$ is precisely the equivalence class

$$\frac{a}{b} = \{(c,d) : c,d \in \mathbb{Z}, d \neq 0, ad = bc\}.$$

Using this idea, an integer $n \in \mathbb{Z}$ does not equal to the fraction $n/1 \in \mathbb{Q}$ since n is an integer and $n/1$ is an infinite set of ordered pairs of integers. Rather, we have the ring homomorphism

$$\phi : \mathbb{Z} \to \mathbb{Q} \quad \text{where} \quad \phi : n \mapsto n/1.$$

As such, we write $\mathbb{Z} \subseteq \mathbb{Q}$ by identifying $\mathbb{Z}$ with $\phi(\mathbb{Z})$.

Theorem 3.1 (fundamental theorem of field theory). If $f(x) \in F[x]$ is irreducible, then

$$\text{there exists an extension field } F \subseteq L \text{ and } \alpha \in L \quad \text{such that} \quad f(\alpha) = 0.$$

Example 3.3. Let $f(x) = x^2 + 1 \in \mathbb{Q}[x]$, where $\mathbb{Q}[x]$ refers to the set of polynomials with rational coefficients. Viewing $f(x)$ as an element of $L[x] = \left(\mathbb{Q}[x] / \left(x^2+1\right)\right)[x]$, we have

$$\begin{aligned} f\left(x + \left(x^2+1\right)\right) &= \left(x + \left(x^2+1\right)\right)^2 + 1 \\ &= x^2 + 2x\left(x^2+1\right) + \left(x^2+1\right)^2 + 1 \\ &= x^2 + 1 + \left(x^2+1\right) \quad \text{by ideal absorption} \\ &= \left(x^2+1\right) \quad \text{by ideal absorption} \end{aligned}$$

Recall that $\alpha \in L$ is a root of $f(x)$ if and only if $x - \alpha$ is a factor of $f(x)$. As such, to say that a field L contains all roots of $f(x)$ is the same as saying that

$$f(x) = a_n(x - \alpha_1)\ldots(x - \alpha) \quad \text{where } \alpha_1, \ldots, \alpha_n \in L.$$

Definition 3.3 (complete splitting property). Let $f(x) \in F[x]$ and $F \subseteq L$ is a field extension. If

$$f(x) = a_n(x - \alpha_1)\ldots(x - \alpha_n) \quad \text{where } \alpha_1, \ldots, \alpha_n \in L,$$

then f splits completely over L.

Theorem 3.2 (Kronecker). Let F be a field and $f(x) \in F[x]$ be a polynomial of degree $n > 0$. Then,

$$\text{there exists a field extension } F \subseteq L \quad \text{such that} \quad f \text{ splits completely over } L.$$

Kronecker's theorem (Theorem 3.2) effectively shows that for any polynoml $f(x) \in F[x]$, f splits completely in some field extension of F. One can prove this result using induction, where the variable involved is n, the degree of f.

Definition 3.4 (algebraic and transcendental elements). An element α is algebraic over F if $f(\alpha)=0$ for some $f(x)\in F[x]$. If α is not algebraic over F, then α is transcendetal over F.

Example 3.4. $\sqrt{2}\in\mathbb{R}$ is algebraic over $\mathbb{Q}$ since $\sqrt{2}$ is a root of $x^2-2\in\mathbb{Q}[x]$.

Example 3.5. $\zeta_n=e^{2\pi i/n}\in\mathbb{C}$ is algebraic over $\mathbb{Q}$ since it is a root of $x^n-1\in\mathbb{Q}[x]$. ζ_n is known as an n^{th} root of unity since raising it to the power of n yields 1. Equivalently, we can think of this as a complex number on an Argand diagram of distance 1 from the origin. We will see this again when we encounter cyclotomic polynomials.

Example 3.6 (Lindemann-Weierstrass theorem). e and π are transcendental over $\mathbb{Q}$, but this is not easy to prove.

Example 3.7. We claim that $\sqrt{2}+\sqrt{3}$ is algebraic over $\mathbb{Q}$. To see why, consider the polynomial

$$\left(x-\sqrt{2}-\sqrt{3}\right)\left(x-\sqrt{2}+\sqrt{3}\right)\left(x+\sqrt{2}-\sqrt{3}\right)\left(x+\sqrt{2}+\sqrt{3}\right),$$

for which upon expansion yields x^4-10x^2+1. So, $\sqrt{2}+\sqrt{3}$ is the root of a non-constant polynomial in $\mathbb{Q}[x]$.

Example 3.8 (Cox p. 80 Question 1). Let $\alpha\in L\backslash\{0\}$ be algebraic over a subfield F. Prove that

$$\frac{1}{\alpha}\quad\text{is also algebraic over } F.$$

Solution. Since α is algebraic over F, then there exists a polynomial $f\in F[x]$ such that $f(\alpha)=0$. Define g to be the polynomial $x^nf(1/x)$, where $n=\deg(f)$. To see why g is still a polynomial, consider

$$f(x)=a_0+a_1x+\ldots+a_nx^n \quad\text{so}\quad x^nf\left(\frac{1}{x}\right)=x^n\left[a_0+a_1\left(\frac{1}{x}\right)+\ldots+a_n\left(\frac{1}{x}\right)^n\right]$$
$$=a_n+a_{n-1}x+\ldots+a_1x^{n-1}+a_0x^n$$

We have $g(1/\alpha)=f(\alpha)/\alpha^n=0$ since $f(\alpha)=0$ which shows that $1/\alpha$ is algebraic over F. □

Definition 3.5 (algebraically closed field). A field K is algebraically closed if all elements α which are algebraic over K are already in K, i.e.

$$\text{all polynomials } f(x)\in K[x]\quad\text{split completely over } K.$$

Example 3.9. $\mathbb{C}$ is a classic example of an algebraically closed field. On the other hand, $\mathbb{R}$ is not algebraically closed. To see why, it suffices to find

$$\text{a polynomial equation } \mathbb{R}[x]\ni p(x)=0\quad\text{that}\quad\text{do not have solutions in } \mathbb{R}.$$

An example of a polynomial equation is $x^2+1=0$.

In fact, $\mathbb{C}$ being algebraically closed is a consequence of the fundamental theorem of algebra.

Definition 3.6 (algebraic closure)**.** Let $F \subseteq K$ be a field extension of a field F. Then, K is an algebraic closure of F if

$$\text{every element in } K \text{ is algebraic over } F \quad \text{and} \quad K \text{ is algebraically closed.}$$

Example 3.10. $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$ as $\mathbb{C}$ is algebraically closed and every element in $\mathbb{C}$ is algebraic over $\mathbb{R}$. For the latter, say $z_0 = a+bi$ is the root of a polynomial $f(x) \in \mathbb{R}[x]$. By the conjugate root theorem, $z_0^* = a-bi$ is also a root.

By Vieta's formula (or the usual expansion), we have

$$(x-z_0)(x-z_0^*) = x^2 - (z_0+z_0^*) + z_0z_0^* = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x].$$

It can be shown, using Zorn's lemma (equivalent to axiom of choice), that the algebraic closure of a field F exists. In other words, given $f(x) \in F[x]$, we may regard it as a polynomial in $K[x]$. Since K is algebraically closed, then $f(x)$ splits completely over K. In fact, this yields another proof of Kronecker's theorem (Theorem 3.2)!

When $\alpha \in L$ is algebraic over F, there many be many non-constant polynomials in $F[x]$ with α as a root. One of these polynomials is especially nice, and it is known as the minimal polynomial.

Definition 3.7 (minimal polynomial)**.** Let $\alpha \in L$ be algebraic over F. Then, define the minimal polynomial to be the unique, non-constant monic polynomial $p \in F[x]$ with the following two properties:

(i) α is a root of p, i.e. $p(\alpha) = 0$

(ii) if $f \in F[x]$ is any polynomial with α as a root, then f is a multiple of p

Besides the characterisation given in Definition 3.7, there are other ways to think about the minimal polynomial. For example,

$$\begin{aligned} f = p \quad & \text{if and only if} \quad f \text{ is a polynomial of minimal degree satisfying } f(\alpha) = 0 \\ & \text{if and only if} \quad f \text{ is irreducible over } F \text{ and } f(\alpha) = 0 \end{aligned}$$

Example 3.11. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is x^2-2. This follows from the irrationality of $\sqrt{2}$, which implies that $\sqrt{2}$ cannot be the root of a polynomial of degree 1 in $\mathbb{Q}[x]$.

Example 3.12. Recall Example 3.7, where we mentioned that

$$\sqrt{2}+\sqrt{3} \quad \text{is} \quad \text{a root of } x^4 - 10x^2 + 1.$$

Is this the minimal polynomial? Well, one way to check is to verify whether $x^4 - 10x^2 + 1$ is irreducible over $\mathbb{Q}$. The easiest way to check for irreducibility is by computer (a manual check using Eisenstein's criterion fails here).

Example 3.13 (cyclotomic polynomial)**.** The minimal polynomial of $\zeta_n = e^{2\pi i/n}$ over $\mathbb{Q}$ is called the n^{th} cyclotomic polynomial and is denoted by $\Phi_n(x)$.

We next show how to describe some interesting subrings and subfields of a given extension $F \subseteq L$. Given $\alpha_1, \ldots, \alpha_n \in L$, we define

$$F[\alpha_1, \ldots, \alpha_n] = \{h(\alpha_1, \ldots, \alpha_n) : h \in F[x_1, \ldots, x_n]\}.$$

So, $F[\alpha_1, \ldots, \alpha_n]$ consists of all polynomial expressions in L that can be formed using $\alpha_1, \ldots, \alpha_n$ with coefficients in F. Then, let

$$F(\alpha_1, \ldots, \alpha_n) = \left\{\frac{\alpha}{\beta} : \alpha, \beta \in F[\alpha_1, \ldots, \alpha_n], \beta \neq 0\right\}.$$

So, $F(\alpha_1, \ldots, \alpha_n)$ is the set of all rational expressions in the α_i with coefficients in F. We can characterise $F(\alpha_1, \ldots, \alpha_n)$ as follows:

Lemma 3.1. $F(\alpha_1, \ldots, \alpha_n)$ is the smallest subfield of the field L containing F and $\alpha_1, \ldots, \alpha_n$.

Since $F(\alpha_1, \ldots, \alpha_n)$ is a subfield of L containing F, we obtaining the following:

$$F \subseteq F(\alpha_1, \ldots, \alpha_n) \subseteq L.$$

So, $F(\alpha_1, \ldots, \alpha_n)$ is obtained from F by adjoining $\alpha_1, \ldots, \alpha_n \in L$. We can use this to construct new fields. Moreover, Lemma 3.1 implies that we can adjoin elements to a field in stages. To be precise, we have the following corollary:

Corollary 3.1. If $F \subseteq L$ and $\alpha_1, \ldots, \alpha_n \in L$, then

$$F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_r)(\alpha_{r+1}, \ldots, \alpha_n) \quad \text{for all } 1 \leq r \leq n-1.$$

Example 3.14. Consider the polynomial $x^4 - 2 \in \mathbb{Q}[x]$. Over $\mathbb{C}$, this polynomial factors as

$$x^4 - 2 = \left(x - \sqrt[4]{2}\right)\left(x + \sqrt[4]{2}\right)\left(x - i\sqrt[4]{2}\right)\left(x + i\sqrt[4]{2}\right).$$

since the roots of $x^4 - 2$ are $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. As such,

$$\mathbb{Q}\left(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\right) \quad \text{is the smallest field over which } x^4 - 2 \text{ splits completely.}$$

This is in fact an example of a splitting field (will learn this in Definition 4.1). In fact, we have *too many elements* in our new field, and it turns out we can describe this field more compactly by only adjoining 2 elements from $\mathbb{Q}$, i.e.

$$\mathbb{Q}\left(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\right) = \mathbb{Q}\left(i, \sqrt[4]{2}\right).$$

To see why, let

$$K = \mathbb{Q}\left(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\right) \quad \text{and} \quad L = \mathbb{Q}\left(i, \sqrt[4]{2}\right).$$

We need to prove $K \subseteq L$ and $L \subseteq K$. The first inclusion follows since $\mathbb{Q} \subseteq L$ is a field extension and $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2} \in L$. Next, we prove the other inclusion $L \subseteq K$. This is obvious — note that $i \in L$, but i can also be written in the following manner:

$$i = \frac{i\sqrt[4]{2}}{\sqrt[4]{2}} \quad \text{which is the quotient of two elements from } K.$$

In fact, field operations permit us to do this. By the closure property, $i \in K$ as well. However, we still need to ascertain that K contains $\mathbb{Q}$ and $\sqrt[4]{2}$. K containing $\mathbb{Q}$ is obvious since $\mathbb{Q} \subseteq K$ is a field extension; showing that K contains $\sqrt[4]{2}$ is very similar to showing that K contains i. It follows that $L \subseteq K$, so $K = L$.

We see how Corollary 3.1 is useful, i.e. adjoining elements to some field in stages.

Example 3.15. By Corollary 3.1, we have

$$\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt{3}\right).$$

As such, we have the following chain of inclusions:

$$\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$$

which shows that we get $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ by first adjoining $\sqrt{2}$ to $\mathbb{Q}$, then adjoining $\sqrt{3}$ to $\mathbb{Q}\left(\sqrt{2}\right)$.

Lemma 3.2. Assume that $F \subseteq L$ is a field extension, and let $\alpha \in L$ be algebraic over F with minimal polynomial $p \in F[x]$. Then, there exists a unique ring isomorphism

$$F[\alpha] \cong F[x]/(p) \quad \text{that is the identity on } F$$

and maps α to the coset $x + (p)$.

Proposition 3.1. Suppose $F \subseteq L$ is a field extension and let $\alpha \in L$. Then,

$$\alpha \text{ is algebraic over } F \quad \text{if and ly if} \quad F[\alpha] = F(\alpha).$$

Proposition 3.2. Let $F \subseteq L$ be a field extension and let $\alpha_1, \ldots, \alpha_n \in L$ be algebraic over F. Then,

$$F[\alpha_1, \ldots, \alpha_n] = F(\alpha_1, \ldots, \alpha_n).$$

Example 3.16. Consider $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$. By Proposition 3.2, this field is equal to $\mathbb{Q}\left[\sqrt{2},\sqrt{3}\right]$, i.e.

$$\text{every element of } \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) \quad \text{is} \quad \text{a polynomial in } \sqrt{2},\sqrt{3} \text{ with rational coefficients.}$$

Since

$$\left(\sqrt{2}\right)^{2n} = 2^n \quad \text{and} \quad \left(\sqrt{2}\right)^{2n+1} = 2^n\sqrt{2} \quad \text{and}$$
$$\left(\sqrt{3}\right)^{2n} = 3^n \quad \text{and} \quad \left(\sqrt{3}\right)^{2n+1} = 3^n\sqrt{3}$$

then

$$Q\left(\sqrt{2},\sqrt{3}\right)=\left\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}:a,b,c,d\in\mathbb{Q}\right\}.$$

In fact, this representation is unique. This will be formally covered once we introduce Definition 3.10 on the degree of a field extension. Just to jump the gun, the uniqueness property comes from the fact that

$$\left\{1,\sqrt{2},\sqrt{3},\sqrt{6}\right\} \quad \text{forms} \quad \text{a basis for } \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) \text{ over } \mathbb{Q}$$

so any element of the field can be uniquely expressed as $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$.

Definition 3.8 (number field)**.** A field of the form

$$\mathbb{Q}\left(\alpha_1,\ldots,\alpha_n\right) \quad \text{where} \quad \alpha_1,\ldots,\alpha_n \text{ are algebraic over } \mathbb{Q}$$

is called a number field.

Number fields are not explicitly covered in this course. Although we will encounter them in MA5202, it turns out that some of the fields that we have encountered so far are number fields, i.e. $\mathbb{Q}\left(i,\sqrt[4]{2}\right)$ and $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$. I recommend Daniel Marcus' book on 'Number Fields' for more insight into this.

3.2. *The Fundamental Theorem of Algebra*

Theorem 3.3. The following are equivalent:

(i) Every non-constant $f(x)\in\mathbb{C}[x]$ has at least one root in $\mathbb{C}$

(ii) Every non-constant $f(x)\in\mathbb{C}[x]$ splits completely over $\mathbb{C}$

(iii) Every non-constant $f(x)\in\mathbb{R}[x]$ has at least one root in $\mathbb{C}$

Theorem 3.4. Every $f(x)\in\mathbb{R}[x]$ of odd degree has at least one root in $\mathbb{R}$.

Lemma 3.3. Every quadratic polynomial in $\mathbb{C}[x]$ splits over $\mathbb{C}$.

Theorem 3.5 (fundamental theorem of algebra)**.** Every non-constant $f(x)\in\mathbb{C}[x]$ splits completely over $\mathbb{C}$.

There are numerous proofs of the fundamental theorem of algebra. For example, Liouville's theorem in Complex Analysis provides a concise proof. The proof provided in Cox's book hinges on the first three results mentioned in this section. In particular, it is worth mentioning that the proof of Theorem 3.4 involves the intermediate value theorem (accompanied with the triangle inequality). Since the IVT depends on the completeness of $\mathbb{R}$, one can argue that the fundamental theorem of algebra is really a theorem in Real Analysis.

Example 3.17 (Trinity College Dublin Michaelmas 2013)**.** Use the fundamental theorem of algebra to show that a non-constant polynomial with real coefficients is irreducible over $\mathbb{R}$ if and only if it is either a polynomial of the form $ax+b$ with $a \neq 0$ or a quadratic polynomial of the form ax^2+bx+c with $a \neq 0$ and $b^2 < 4ac$.

Solution. The backward direction is obvious — f we have a linear polynomial $ax+b$ with $a \neq 0$, then its factors are of degree zero and one so it is already irreducible. If the polynomial is quadratic and we assume that its discriminant $\Delta < 0$, then the equation $ax^2+bx+c=0$ has no roots in $\mathbb{R}$ and hence, irreducible over $\mathbb{R}$.

For the forward direction, we now assume that $p(x)$ is a non-constant polynomial with real coefficients but irreducible over $\mathbb{R}$. As a corollary of the fundamental theorem of algebra, $p(x)$ has at least one root in $\mathbb{C}$. Call this root α.

Note that $\mathbb{R} \subseteq \mathbb{C}$. If $\alpha \in \mathbb{R}$, then $x-\alpha$ is a factor of $p(x)=0$ in the polynomial ring $\mathbb{R}[x]$, where we define $\mathbb{R}[x]$ to be the set of polynomials with real coefficients. Hence, $p(x)=a(x-\alpha)$, where a is the leading coefficient of $p(x)$. Setting $b=-a\alpha$ and then, we are done for the case of a linear polynomial. If α contains an imaginary part, then $\alpha \in \mathbb{C}$ and also, $\alpha^* \in \mathbb{C}$. If we define $\alpha = p+qi$ for $p,q \in \mathbb{R}$, note that

$$(x-\alpha)(x-\alpha^*) = x^2-(\alpha+\alpha^*)x+\alpha\alpha^* = x^2+2px+p^2+q^2,$$

which is a quadratic polynomial in $\mathbb{R}[x]$. However, $p(x)$ is irreducible over $\mathbb{R}$, which implies that $a(x^2+2px+p^2+q^2)=0$ has no roots in $\mathbb{R}$. Setting a,b,c where appropriate, the other result follows. □

3.3. *Irreducible Polynomials*

Since minimal polynomials are irreducible, it hints that irreducibility plays an important role in Field Theory. However, given an arbitrary polynomial $f \in F[x]$, it may not be obvious that f is irreducible. We shall provide some methods to determine whether a polynomial is irreducible, which are namely

corollary of Gauss' lemma and Eisenstein's criterion and mod p irreducibility test.

As a consequence of Gauss' lemma (MA3201), we have the following corollary:

Corollary 3.2. Let $f \in \mathbb{Z}[x]$ be of degree > 0 and is reducible over $\mathbb{Q}$. Then,

$$\text{there exist } g,h \in \mathbb{Z}[x] \text{ where } \deg(g), \deg(h) < \deg(f) \quad \text{such that} \quad f = gh.$$

Proof. Suppose f is reducible in $\mathbb{Q}[x]$, then $f = g_1 h_1$, where $g_1, h_1 \in \mathbb{Q}[x]$ have degrees $< \deg(f)$. By Gauss' lemma,

$$\text{there exists } \delta \in Q \quad \text{such that} \quad g = \delta g_1 \text{ and } h = \delta^{-1} h_1 \text{ have integer coefficients.}$$

Then, $f = gh$ is the desired factorisation. □

Theorem 3.6. Let $n = \deg(f) > 0$. First, note that if $f(i) = 0$ for some $0 \leq i \leq n-1$, then $x - i$ is a factor of f and we can quit. Hence, when performing the algorithm, we may assume that $f(0), \ldots, f(n-1)$ are nonzero. Then create a set of polynomials as follows:

1. Fix an integer $0 < d < n$.
2. Fix divisors $a_0, \ldots, a_d \in \mathbb{Z}$ of $f(0), \ldots, f(d) \in \mathbb{Z}$.
3. Use Lagrange interpolation to construct a polynomial $g \in \mathbb{Q}[x]$ of degree $\leq d$ such that $g(i) = a_i$ for $i = 0, \ldots, d$.
4. Accept g if it has degree d and integer coefficients; reject it otherwise.

Doing this for all $0 < d < n$ and all divisors $a_0 \mid f(0), \ldots, a_d \mid f(d)$ gives a set of polynomials $g \in \mathbb{Z}[x]$. Then, the set of polynomials $g \in \mathbb{Z}[x]$ is finite, and

$$f \text{ is irreducible over } \mathbb{Q} \quad \text{if and only if} \quad \text{it is not divisible by any of the polynomials in this set.}$$

Theorem 3.7 (Eisenstein's criterion)**.** Let

$$f(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + a_n x^n \in \mathbb{Z}[x].$$

Suppose there exists a prime p such that the following occur:

(i) $p \mid a_i$ for all $0 \leq i \leq n-1$

(ii) p does not divide a_n

(iii) p^2 does not divide a_0

Then, $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. Suppose on the contrary that $f(x)$ is reducible over $\mathbb{Q}$. Then,

$$\text{there exist } g, h \in \mathbb{Z}[x] \quad \text{sucht that} \quad f = gh \text{ and } \deg(g) \geq 1 \text{ and } 1 \leq \deg(h) < n.$$

We can set

$$g(x) = b_0 + \ldots + b_r x^r \text{ and } h(x) = c_0 + \ldots + c_s x^s,$$

so this implies that $r \geq 1$ and $1 \leq s < n$. Since $p \mid a_0$ but p^2 does not divide a_0 and $a_0 = b_0 c_0$, then by Euclid's lemma, $p \mid b_0$ or $p \mid c_0$. Suppose $p \mid b_0$ but p does not divide c_0. We note that $a_n = b_r c_s$. As

$$p \text{ does not divide } a_n \quad \text{then} \quad p \text{ does not divide } b_r c_s.$$

So, p does not divide b_r. As such, there exists a least $t \in \mathbb{Z}$ such that p does not divide b_t.

Since

$$\begin{aligned} a_0 &= b_0c_0 \\ a_1 &= b_0c_1 + b_1c_0 \\ a_2 &= b_0c_2 + b_1c_1 + b_2c_0 \end{aligned}$$

we can infer that

$$a_t = b_0c_t + \ldots + b_{t-1}c_1 + b_tc_0.$$

As $p \mid a_t$, by the choice of t, $b_0c_t, b_1c_{t-1}, \ldots, b_{t-1}c_1$ are all divisible by p. This forces b_tc_0 to be a multiple of p as well. However, this is a contradiction because p neither divides b_t nor c_0. □

Example 3.18. Let

$$f(x) = x^n + px + p \quad \text{where } n \geq 2 \text{ and } p \text{ is prime.}$$

By Eisenstein's criterion for the prime p, it immediately implies that f is irreducible over $\mathbb{Q}$ regardless of our choice of n.

Example 3.19 (Trinity College Dublin Michaelmas 2013)**.** Using Eisenstein's criterion, or otherwise, prove that $\sqrt{3}$ is irrational, and is not of the form $b\sqrt{2}$ for any $b \in \mathbb{Q}$. Hence or otherwise, show that there cannot exist rational numbers a and b such that $\sqrt{3} = a + b\sqrt{2}$ and thus prove that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

Solution. We first prove that $\sqrt{3}$ is irrational. Consider the polynomial $f(x) = x^2 - 3$, for which its roots are $\pm\sqrt{3}$. It suffices to prove that the equation $f(x) = 0$ is irreducible over $\mathbb{Q}$ as seen from the fact that $f(x)$ cannot be split into linear factors. We use Eisenstein's criterion. Set $p = 3$. Then, $3 \mid 3$, $3 \mid 0$ but 3 does not divide 1. Also, $3^2 = 9$ does not divide -3. It follows that $\sqrt{3}$ is irrational.

For the next part, consider the polynomial $2x^2 - 3$ and again, it is easy to show by Eisenstein's criterion that it is irreducible over $\mathbb{Q}$.

For the last part, suppose on the contrary that there exist $a, b \in \mathbb{Q}$ such that $\sqrt{3} = a + b\sqrt{2}$. So,

$$a^2 + 2b^2 + 2ab\sqrt{2} = 3 \quad \text{which implies} \quad 2ab\sqrt{2} = 3 - a^2 - 2b^2$$

The LHS is irrational but the RHS is rational, which is a contradiction! Now, we prove that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Recall that the quadratic field $\mathbb{Q}(\sqrt{2})$ is the set of numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$. Since we showed that there does not exist $a, b \in \mathbb{Q}$ such that $\sqrt{3} = a + b\sqrt{2}$, then the result follows. □

Definition 3.9 (cyclotomic polynomial)**.** Let p be a prime. We define the p^{th} cyclotomic polynomial, $\Phi_p(x)$, to be

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = \sum_{i=0}^{p-1} x^i.$$

In Definition 3.9, we mentioned that the index is some prime p. In general, this can be replaced with some arbitrary positive integer n. As a corollary of Eisenstein's criterion (Theorem 3.7), we have the following result:

Corollary 3.3. For any prime p, $\Phi_p(x)$ is irreducible over $\mathbb{Q}$.

Before we prove Corollary 3.3, we give a remark that Eisenstein's criterion can be used to determine the minimal polynomial of the p^{th} root of unity $\zeta_p = e^{2\pi i/p}$, where p is prime. Note that

$$x^p - 1 = (x-1)\left(x^{p-1} + \ldots + x + 1\right) \quad \text{so} \quad \zeta_p \text{ is a root of } \Phi_p.$$

Proving Corollary 3.3 will in turn show that the minimal polynomial of ζ_p over $\mathbb{Q}$ is $x^{p-1} + \ldots + x + 1$. We now prove Corollary 3.3.

Proof. The trick is to consider $\Phi_p(x+1)$ instead. Let this be denoted by $f(x)$. Then,

$$f(x) = \Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \ldots + \binom{p}{p-1}.$$

It is a well-known result that $\binom{p}{k}$ is divisible by p for $1 \le k \le p-1$. This is because

$$\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k!}$$

and since

$$k! = k(k-1)(k-2)\cdot\ldots\cdot 3\cdot 2\cdot 1 \quad \text{with} \quad \text{none of these products dividing } p,$$

the result follows. So for f, every coefficient except that of x^{p-1} is divisible by p and the constant term $\binom{p}{p-1} = p$ is not divisible by p^2. By Eisenstein's criterion, f is irreducible over $\mathbb{Q}$, so Φ_p is irreducible over $\mathbb{Q}$. □

Our last irreducibility criterion is known as the mod p irreducibility test.

Theorem 3.8 (mod p irreducibility test). Let p be a prime and suppose $f(x) \in \mathbb{Z}[x]$ with $\deg(f) \ge 1$. Let $\overline{f}(x) \in \mathbb{Z}_p[x]$ be obtained from $f(x)$ by reducing all the coefficients of $f(x)$ mod p. If

$$\overline{f} \text{ is irreducible over } \mathbb{Z}_p \text{ and } \deg(f) = \deg\left(\overline{f}\right) \quad \text{then} \quad f \text{ is irreducible over } \mathbb{Q}.$$

Example 3.20. Let $f(x) = 21x^3 - 3x^2 + 2x + 9$. Then, over $\mathbb{Z}_2$, we have $\overline{f}(x) = x^3 + x^2 + 1$. We see that $\overline{f}(0) = 1$ and $\overline{f}(1) = 1$, so $\overline{f}(x)$ is irreducible over $\mathbb{Z}_2$, which implies that $f(x)$ is irreducible over $\mathbb{Q}$.

Proposition 3.3. Let p be a prime. Then,

$$f = x^p - a \in F[x] \text{ is irreducible over } F \quad \text{if and only if} \quad f \text{ has no roots in } F.$$

Example 3.21. Let F be a subfield of $\mathbb{R}$ and let p be an odd prime. Given $a \in F$, define $\sqrt[p]{a}$ to be the real p^{th} root of a. Furthermore, since p is odd, then $\sqrt[p]{a}$ is the only real p^{th} root of a. To see why, suppose there exists another real p^{th} root of a. Then, consider the complex number

$$e^{2k\pi i/p} \cdot \sqrt[p]{a} \quad \text{where } p \text{ is prime and } 0 \leq k \leq p.$$

For this root to lie on the real axis, we must have $2k\pi/p = \pi$, so $2k = p$. However, p is odd, so it cannot take the form $2k$ for any $k \in \mathbb{Z}$.

Returning to the question on irreducibility, by Proposition 3.3,

$$x^p - a \text{ is irreducible over } F \quad \text{if and only if} \quad \sqrt[p]{a} \notin F.$$

Example 3.22 (Cox p. 88 Question 9)**.** Let k be a field, and let

$$F = k(t) \quad \text{be} \quad \text{the field of rational functions in } t \text{ with coefficients in } k.$$

Then consider $f = x^p - t \in F[x]$, where p is prime. Prove that f has no roots in F, which in turn by Proposition 3.3, would imply that f is irreducible over F.

Solution. Suppose on the contrary that f is reducible over F. Then, $r \in F = k(t)$ is a root of $f(x)$. As such, $r^p = t$. This implies that

$$r = \frac{g(t)}{h(t)} \quad \text{where } g(t), h(t) \in k[t] \text{ and } h(t) \neq 0.$$

Moreover, we can assume that $\gcd(g,h) = 1$. Hence, $(g(t))^p = t(h(t))^p$. This implies that $(h(t))^p \mid (g(t))^p$, so $h(t) \mid t(t)$ in $k[t]$ since $k[t]$ is a UFD (recall from MA3201 that if F is a field then $F[x]$ is a UFD).

Since $\gcd(g,h) = 1$, then $h(t) \mid 1$, meaning that h is a constant polynomial. As such, let $h(t) = c$, where c is non-zero. Then,

$$r = \frac{g(t)}{c} \quad \text{so} \quad r^p = \frac{(g(t))^p}{c^p}.$$

Since $r^p = t$, then $(g(t))^p = c^p t$. As such, $g(t) \mid t$, so there exists $g_1(t) \in k[t]$ such that $g(t) = tg_1(t)$. Substituting this back, we obtain $t^p (g_1(t))^p = c^p t$. Since $t \neq 0$ in $k(t)$, cancelling t on both sides yields

$$t^{p-1} (g_1(t))^p = c^p.$$

Since the LHS is divisible by t^{p-1} whereas the RHS is a non-zero constant c^p, this yields a contradiction unless $t = 0$, which cannot occur in $k(t)$. □

3.4. *The Degree of an Extension*

Suppose F and L are two fields, with L being an extension of F. Recall that this is the same as saying that F is a subfield of L. So far, there is one bit of structure that has not been utilised. We also recall that any field is an Abelian group under addition — in particular, L has this property. Moreover, since $F \subseteq L$, the ability to multiply elements of L implies that we can

$$\text{multiply elements of } F \quad \text{times} \quad \text{elements of } L.$$

This yields a scalar multiplication property, for which one can check using tools from MA2101 that L becomes a vector space over F. Analogous to the concept of rank in MA2001/MA2101, we have the following definition regarding the degree of a field extension.

Definition 3.10 (degree of extension)**.** Let $F \subseteq L$ be a field extension. Then,

$$L \text{ is a finite extension of } F \quad \text{if} \quad L \text{ is a finite-dimensional vector space over } F.$$

The degree of L over F, denoted by $[L:F]$, is defined as follows:

$$[L:F] = \begin{cases} \dim_F L & \text{if } L \text{ is a finite extension of } F; \\ \infty & \text{otherwise.} \end{cases}$$

Example 3.23. For $\mathbb{R} \subseteq \mathbb{C}$, the usual way of writing complex numbers as $a+bi$ shows that 1 and i forms a basis of $\mathbb{C}$ as a vector space over $\mathbb{R}$. In other words,

$$\{1,i\} \quad \text{is an } \mathbb{R}\text{-basis for } \mathbb{C}.$$

So, $[\mathbb{C}:\mathbb{R}] = 2$. In fact, an obvious reason why the degree of the extension is 2 is attributed to Proposition 3.4, but we shall briefly state why. It is simply because

$$\mathbb{C} = \mathbb{R}(i) \quad \text{and} \quad \text{the minimal polynomial of } i \text{ over } \mathbb{R} \text{ is } x^2+1.$$

Example 3.24. $[\mathbb{R}:\mathbb{Q}] = \infty$ since any finite-dimensional vector space over $\mathbb{Q}$ is countable but any over $\mathbb{R}$ is uncountable.

We have an obvious characterisation of extensions of degree 1.

Lemma 3.4. An extension $F \subseteq L$ has

$$\text{degree } [L:F] = 1 \quad \text{if and only if} \quad F = L.$$

Proof. The reverse direction is obvious. To prove the forward direction, say $[L:F] = 1$, then any non-zero element of L, say $1 \in L$, is a basis. Thus, $L = \{a \cdot : a \in F\} = F$. □

In general, we can compute the degree of an extension $F \subseteq F(\alpha)$ as follows:

Proposition 3.4 (computing degree of extension)**.** Suppose $F \subseteq L$ is an extension and $\alpha \in L$. Then, the following hold:

(i) α is algebraic over F if and only if $[F(\alpha) : F] < \infty$

(ii) If α is algebraic over F and n is the degree of the minimal polynomial of α over F, then

$$\left\{1, \alpha, \ldots, \alpha^{n-1}\right\} \text{ forms a basis of } F(\alpha) \text{ over } F \quad \text{and consequently} \quad [F(\alpha) : F] = n.$$

As such, Proposition 3.4 implies that when the minimal polynomial of α has degree n, then every $\beta \in F(\alpha)$ can be uniquely written as

$$\beta = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \quad \text{where } a_0, \ldots, a_{n-1} \in F.$$

Example 3.25. Consider the extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}\right)$. Since the minimal polynomial of $\sqrt{2}$ is $x^2 - 2$, by Proposition 3.4, we have

$$\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2 \quad \text{and} \quad \mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}.$$

In fact, this representation of $\mathbb{Q}\left(\sqrt{2}\right)$ is unique.

Example 3.26. Recall Example 3.7, where we mentioned that the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ is $x^4 - 10x^2 + 1$. So, $\left[\mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right) : \mathbb{Q}\right] = 4$, and every $\beta \in \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$ can be uniquely written as

$$\beta = a + b\left(\sqrt{2} + \sqrt{3}\right) + c\left(\sqrt{2} + \sqrt{3}\right)^2 + d\left(\sqrt{2} + \sqrt{3}\right)^3 \quad \text{where } a, b, c, d \in \mathbb{Q}.$$

We will see in Example 3.28 that there is a neat derivation that $\left[\mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right) : \mathbb{Q}\right] = 4$ using the tower theorem (Theorem 3.9). Just to jump the gun,

$$\text{the fields} \quad \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right) \text{ and } \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \quad \text{are equivalent.}$$

This is not obvious, but we will establish it in Example 3.28. Since

$$\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt{3}\right),$$

we can use the tower theorem (Theorem 3.9) to deduce that the degree of the field extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$ is 4. More to come in due course.

Example 3.27. Let $F(x)$ be the field of rational functions in the variable x with coefficients in F. Then, $[F(x) : F] = \infty$ since x is not algebraic over F.

As mentioned earlier, we can determine how the degree behaves when we have successive extensions $F \subseteq K \subseteq L$ using the tower theorem (Theorem 3.9).

Theorem 3.9 (tower theorem)**.** Suppose we have fields $F \subseteq K \subseteq L$. Then, the following hold:

(a) If $[K : F] = \infty$ or $[L : K] = \infty$, then $[L : F] = \infty$

(b) If $[K:F]<\infty$ and $[L:K]<\infty$, then $[L:F]=[L:K][K:F]$.

We will only prove **(b)**.

Proof. Let $X=\{x_1,\ldots,x_n\}$ be a basis for L over K and $Y=\{y_1,\ldots,y_m\}$ be a basis for K over F. Define YX to be the following set:

$$YX=\left\{y_jx_i : 1\le j\le m, 1\le i\le n\right\}$$

It suffices to show that YX is a basis for L over F.

Let $a\in L$. Then, there exist $b_1,\ldots,b_n\in K$ such that

$$a=\sum_{i=1}^{n} b_ix_i.$$

Also, for each $1\le i\le n$, there exist $c_{i1},\ldots,c_{im}\in F$ such that

$$b_i=\sum_{j=1}^{m} c_{ij}y_j.$$

As such,

$$a=\sum_{i=1}^{n}\left(\sum_{j=1}^{m} c_{ij}y_j\right)x_i=\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}y_jx_i,$$

which proves that YX spans L over F.

Now, suppose there are elements $c_{ij}\in F$ such that

$$\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}y_jx_i=0.$$

Since

$$\sum_{j=1}^{m} c_{ij}y_j\in K$$

and X is a basis for L over K, it implies that for all $1\le i\le n$,

$$\sum_{j=1}^{m} c_{ij}y_j=0.$$

However, each $c_{ij}\in F$ and Y is a basis for E over F, so each $c_{ij}=0$. This shows that YX is linearly independent over F. □

Corollary 3.4 (Cox p. 94 Question 7)**.** Suppose we have extensions $L_0\subset L_1\subset\cdots\subset L_m$. Then, the following hold:

(a) If $[L_i:L_{i-1}]=\infty$ for some $1\le i\le m$, then $[L_m:L_0]=\infty$

(b) If $[L_i : L_{i-1}] < \infty$ for all $1 \leq i \leq m$, then

$$[L_m : L_0] = [L_m : L_{m-1}]\,[L_{m-1} : L_{m-2}] \cdots [L_2 : L_1]\,[L_1 : L_0]$$

Proof. Use induction. □

Example 3.28. We will analyse $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ using

$$\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right).$$

Recall that $\left\{1, \sqrt{2}\right\}$ is a basis for $\mathbb{Q}\left(\sqrt{2}\right)$ over $\mathbb{Q}$ since $x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$. Furthermore, one can show that $x^2 - 3$ is the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}\left(\sqrt{2}\right)$ (remember to justify this), so that $\{1, \sqrt{3}\}$ forms a basis for $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ over $\mathbb{Q}\left(\sqrt{2}\right)$.

By the tower theorem (Theorem 3.9), we have

$$\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2 \cdot 2 = 4.$$

As such, the products of the bases $1, \sqrt{2}$ and $1, \sqrt{3}$, namely $1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3} = \sqrt{6}$ give a basis of $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ over $\mathbb{Q}$.

Recall that $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ span $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ over $\mathbb{Q}$. We now see that these elements form a basis that arises naturally from the tower theorem. We note that

$$\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right) \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$$

where the first inclusion is obvious but the second is not. We shall justify that

$$\mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right) \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \quad \text{is a field extension.}$$

Note that

$$\sqrt{2} + \sqrt{3} \in \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right) \quad \text{so} \quad \frac{1}{\sqrt{2} + \sqrt{3}} = \sqrt{3} - \sqrt{2} \in \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$$

Here, we merely applied a field axiom. In particular, this shows that

$$\left(\sqrt{2} + \sqrt{3}\right) + \left(\sqrt{3} - \sqrt{2}\right) = 2\sqrt{3} \quad \text{which is an element of } \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)!$$

Of course, it follows that $\sqrt{3}$ and $\sqrt{2}$ are elements of $\mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$, so they are also elements of $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. We now give a different proof using the tower theorem. Earlier, we showed that $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right] = 4$, so by the tower theorem (Theorem 3.9), we have

$$\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)\right]\left[\mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right) : \mathbb{Q}\right]$$

which implies

$$\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)\right] = 1 \quad \text{and consequently} \quad \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right).$$

Example 3.29. Let $\omega = e^{2\pi i/3}$ be a third root of unity and $L = \mathbb{Q}\left(\omega, \sqrt[3]{2}\right)$. We shall compute $[L : \mathbb{Q}]$ using the extension fields

$$\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt[3]{2}\right) \subseteq \mathbb{Q}\left(\omega, \sqrt[3]{2}\right) = L.$$

To determine $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right]$, we first observe that $x^3 - 2$ is irreducible over $\mathbb{Q}$. This is an obvious fact as we can solve for the roots easily but we realise that one root is irrational and the other two are *living in the complex world*. Actually, one can also prove this result using Eisenstein's criterion (Theorem 3.7) with $p = 2$. Hence, $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$.

We then compute $\left[L : \mathbb{Q}\left(\sqrt[3]{2}\right)\right]$. By a formula learnt in O-Level or by recognising the presence of a geometric series, we see that

$$x^3 - 1 = (x-1)\left(x^2 + x + 1\right).$$

Recall that $x^2 + x + 1 = 0$ has roots ω and ω^2, neither of which is real. As $\mathbb{Q}\left(\sqrt[3]{2}\right) \subseteq \mathbb{R}$, then $x^2 + x + 1$ has no root in this field, so that $x^2 + x + 1$ is the minimal polynomial of ω over $\mathbb{Q}\left(\sqrt[3]{2}\right)$. As such, $\left[L : \mathbb{Q}\left(\sqrt[3]{2}\right)\right] = 2$ since $L = \mathbb{Q}\left(\sqrt[3]{2}\right)(\omega)$.

By the tower theorem (Theorem 3.9), we can easily conclude that

$$[L : \mathbb{Q}] = \left[L : \mathbb{Q}\left(\sqrt[3]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 2 \cdot 3 = 6.$$

Example 3.30 (Cox p. 94 Question 2)**.** Compute the degrees of the following extensions:

(a) $\mathbb{Q} \subseteq \mathbb{Q}\left(i, \sqrt[4]{2}\right)$

(b) $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}\right)$

(c) $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$

(d) $\mathbb{Q}\left(i, \sqrt{2+\sqrt{2}}\right)$

Solution.

(a) By the tower theorem,

$$\left[\mathbb{Q}\left(i, \sqrt[4]{2}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(i, \sqrt[4]{2}\right) : \mathbb{Q}(i)\right] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = 4 \cdot 2 = 8.$$

(b) Again, by the tower theorem, the degree of the extension is $2 \cdot 3 = 6$.

(c) Consider

$$\left(x - \sqrt{2+\sqrt{2}}\right)\left(x + \sqrt{2+\sqrt{2}}\right) = x^2 - \left(2 + \sqrt{2}\right).$$

As such,

$$\left[\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] \cdot \left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2 \cdot 2 = 4.$$

Alternatively, we can continue from where we left off — set $x^2-\left(2+\sqrt{2}\right)=0$, so $x^2-2=\sqrt{2}$, which implies $x^4-4x^2+2=0$. This is the minimal polynomial of $\sqrt{2+\sqrt{2}}$ over $\mathbb{Q}$, and as it is of degree 4, the required degree of the field extension is 4.

(d) By the tower theorem, applying **(c)** shows that the degree of the extension is $2\cdot 4=8$. □

On page 94 of Cox's textbook, the reader is asked to find a basis over $\mathbb{Q}$ using the method of Example 3.28 for each of the extensions in Example 3.30. This is rather straightforward and we omit the details. Well, as an example for the extension $\mathbb{Q}\subseteq\mathbb{Q}\left(\sqrt[4]{2}\right)$ in **(a)**, the desired basis is

$$\left\{1,\alpha,\alpha^2,\alpha^3,i,i\alpha,i\alpha^2,i\alpha^3\right\}\quad\text{where } \alpha=\sqrt[4]{2}.$$

Example 3.31 (Cox p. 94 Question 4)**.** Suppose

$$F\subseteq L \text{ is a finite extension}\quad\text{with}\quad [L:F] \text{ prime}.$$

(a) Show that the only subfields of L containing F are F and L.

(b) Show that $L=F(\alpha)$ for any $\alpha\in L\backslash F$.

Solution.

(a) By definition, F and L are subfields of L. Since $F\subseteq L$ is a finite extension with the degree of extension being some prime p, we can write

$$p=[L:F(\alpha)]\,[F(\alpha):F]\quad\text{by the tower theorem (Theorem 3.9).}$$

Here, $F\subseteq F(\alpha)$ is a finite extension. So, we can have either $[F(\alpha):F]=1$ or p. If the degree of this extension is 1, then $F=F(\alpha)$ by Lemma 3.4; if the degree of this extension is p, then $L=F(\alpha)$. In either case, we see that the only subfields are F and L.

(b) Since $\alpha\in L$, then $F\subseteq F(\alpha)\subseteq L$. Since $\alpha\notin F$, by **(a)**, $F(\alpha)\neq F$ so it follows that $L=F(\alpha)$. □

Example 3.32 (Cox p. 94 Question 5)**.** Consider the extension $\mathbb{Q}\subseteq L=\mathbb{Q}\left(\sqrt[4]{2},\sqrt[3]{3}\right)$. We will compute $[L:\mathbb{Q}]$.

(a) Show that x^4-2 and x^3-3 are irreducible over $\mathbb{Q}$.

(b) Use $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt[4]{2})\subseteq L$ to show that $4\mid[L:\mathbb{Q}]$ and $[L:\mathbb{Q}]\le 12$.

(c) Use $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt[3]{3})\subseteq L$ to show that $[L:\mathbb{Q}]$ is also divisible by 3.

(d) Explain why parts **(b)** and **(b)** imply that $[L:\mathbb{Q}]=12$. This works because 3 and 4 are relatively prime. Do you see why?

Solution.

(a) Use Eisenstein's criterion for $p=2$ and $p=3$ respectively.

(b) By the tower theorem,

$$[L:\mathbb{Q}]=\left[L:\mathbb{Q}\left(\sqrt[4]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right]=\left[L:\mathbb{Q}\left(\sqrt[4]{2}\right)\right]\cdot 4.$$

The first result follows. For the second result, the minimal polynomial of $\sqrt[3]{3}$ over $\mathbb{Q}\left(\sqrt[4]{2}\right)$ divides x^3-3, so it implies $\left[L:\mathbb{Q}\left(\sqrt[4]{2}\right)\right]\le 3$. Putting this into our equation which made use of the tower theorem yields the desired result.

(c) Similar as **(b)** — use the tower theorem.

(d) From **(b)** and **(c)**, we have $3,4 \mid [L:\mathbb{Q}]$ so $12 \mid [L:\mathbb{Q}]$. Since $[L:\mathbb{Q}] \leq 12$ by **(b)**, the result follows. □

3.5. *Algebraic Extensions*

Definition 3.11 (algebraic extension)**.** A field extension $F \subseteq L$ is

$$\text{algebraic} \quad \text{if every element of } L \text{ is algebraic over } F.$$

Lemma 3.5. Let $F \subseteq L$ be a finite extension. Then, the following hold:

(i) $F \subseteq L$ is algebraic

(ii) if $\alpha \in L$, then

$$\text{the degree of the minimal polynomial of } \alpha \text{ over } F \quad \text{divides } [L:F].$$

Proof. Let $\alpha \in L$, then we obtain the field extension $F \subseteq F(\alpha) \subseteq L$. By the tower theorem, we have

$$[L:F] = [L:F(\alpha)][F(\alpha):F].$$

Since $F \subseteq L$ is a finite extension, then $[L:F]$ is finite, so $[F(\alpha):F]$ is finite and it divides $[L:F]$. The result follows. □

Lemma 3.5 states that every finite extension is algebraic. However, the converse is generally not true, i.e. not every algebraic extension is finite (Example 3.33).

Example 3.33 (Cox p. 98 Question 1)**.** Here, we will show that there exists some algebraic extension which is finite. By definition, the field of algebraic integers $\mathbb{A}$ (Cox uses $\overline{\mathbb{Q}}$) is algebraic over $\mathbb{Q}$. We will show that $[\mathbb{A}:\mathbb{Q}] = \infty$.

To see why, we first establish that for any integer $n \geq 2$, $\mathbb{A}$ has a subfield L such that $[L:\mathbb{Q}] = n$. Recall Example 3.18, where we used Eisenstein's criterion to prove that

$$\text{the polynomial } f(x) = x^n + px + p \quad \text{where } n \geq 2 \text{ and } p \text{ is prime,}$$

is irreducible over $\mathbb{Q}$ regardless of the choice of n. As such, if α is a root of $f(x)$ in $\mathbb{A}$, then $L = \mathbb{Q}(\alpha)$ is a subfield of $\mathbb{A}$. As f is the minimal polynomial of α over $\mathbb{Q}$ and $\deg(f) = n$, it follows that $[L:\mathbb{Q}] = n$. By the tower theorem, we have

$$[\mathbb{A}:\mathbb{Q}] = [\mathbb{A}:L][L:\mathbb{Q}] \quad \text{so} \quad [\mathbb{A}:\mathbb{Q}] = [\mathbb{A}:L] \cdot n.$$

Since n can be made arbitrarily large, it follows that $[\mathbb{A}:\mathbb{Q}] = \infty$.

Theorem 3.10. $\mathbb{A}$ is algebraically closed.

We then explore the structure of finite extensions.

Theorem 3.11. Let $F \subseteq L$ be a field extension. Then,

$$[L:F] < \infty \quad \text{if and only if} \quad \begin{array}{l} \text{there exist } \alpha_1, \ldots, \alpha_m \in L \text{ such that} \\ \text{each } \alpha_i \text{ is algebraic over } F \quad \text{and} \quad L = F(\alpha_1, \ldots, \alpha_m) \end{array}$$

Proposition 3.5 (sum and product of algebraic elements is algebraic)**.** Let $F \subseteq L$ be a field extension. If

$$\alpha, \beta \in L \text{ are algebraic over } F \quad \text{then} \quad \text{so are } \alpha + \beta \text{ and } \alpha\beta.$$

Proof. By Theorem 3.11, $F \subseteq F(\alpha, \beta)$ is a finite extension. Recall from Lemma 3.5 that every finite extension is algebraic. As such, every element of $F(\alpha, \beta)$ is algebraic over F. By field closure properties, we have $\alpha + \beta, \alpha\beta \in F(\alpha, \beta)$, and the result follows. □

Corollary 3.5. Given any field extension $F \subseteq L$, the subset

$$M = \{\alpha \in L : \alpha \text{ is algebraic over } F\} \quad \text{is a subfield of } L \text{ containing } F.$$

Proof. We have

$$F \subseteq M \quad \text{since} \quad a \in F \text{ is a root of } x - a \in F[x]$$

and M is closed under addition and multiplication by Proposition 3.5 since the sum and product of algebraic elements over F are also algebraic over F. Since $-1 \in F \subseteq M$, then $\alpha \in M$ implies $-\alpha = -1 \cdot \alpha \in M$. Finally, if $\alpha \neq 0 \in M$, then $1/\alpha \in M$ (since the reciprocal of any non-zero algebraic element is also algebraic by Example 3.8). Hence, M is a subfield of L. □

Example 3.34. A complex number $z \in \mathbb{C}$ is called an algebraic number if it is algebraic over $\mathbb{Q}$. As such, we obtain the field of algebraic numbers $\mathbb{A}$, defined as follows:

$$\mathbb{A} = \{z \in \mathbb{C} : z \text{ is an algebraic number}\}.$$

Theorem 3.12 (being algebraic is transitive)**.** Let $F \subseteq K \subseteq L$. If $\alpha \in L$ is algebraic over K and K is algebraic over F, then α is algebraic over F.

Example 3.35 (Cox p. 98 Question 5)**.** In 1873 Hermite proved that

$$e \text{ is transcendental over } \mathbb{Q} \quad \text{(Hermite-Lindemann theorem)},$$

and in 1882, Lindemann showed that

$$\pi \text{ is transcendental over } \mathbb{Q} \quad \text{(Lindemann-Weierstrass theorem)}.$$

It is unknown whether $\pi + e$ and $\pi - e$ are transcendental. Prove that at least one of these numbers is transcendental over $\mathbb{Q}$.

Solution. Suppose on the contrary that neither $\pi + e$ nor $\pi - e$ is transcendental. Then, both of them are algebraic, so their sum and difference are also algebraic by Proposition 3.5, i.e.

$$2\pi \text{ and } 2e \quad \text{are algebraic.}$$

It follows that π and e are algebraic over $\mathbb{Q}$, which is a contradiction by the results of Hermite and Lindemann (we can include Weierstrass as well). As such, at least one of $\pi + e$ and $\pi - e$ is transcendental over $\mathbb{Q}$. □

Corollary 3.6. If we have field extensions $F \subseteq K \subseteq L$, where L is algebraic over K and K is algebraic over F, then L is algebraic over F.

Example 3.36. Consider the equation

$$x^{11} - \left(\sqrt{2} + \sqrt{5}\right)x^5 + 3\sqrt[4]{12}x^3 + (1+3i)x + \sqrt[5]{17} = 0.$$

Note that the coefficients are algebraic over $\mathbb{Q}$, so every complex solution of the equation is an algebraic number by Theorem 3.12 (*algebraic property is transitive*).

Example 3.37 (Cox p. 98 Question 2)**.** Let $\alpha \in \mathbb{C}$ be a solution of

$$x^{11} - \left(\sqrt{2} + \sqrt{5}\right)x^5 + 3\sqrt[4]{12}x^3 + (1+3i)x + \sqrt[5]{17} = 0.$$

We will show that the minimal polynomial of α over $\mathbb{Q}$ has degree at most 1760. Let

$$L = \mathbb{Q}\left(\sqrt{2}, \sqrt{5}, \sqrt[4]{12}, i, \sqrt[5]{17}, \alpha\right).$$

(a) Show that $[L : \mathbb{Q}] \leq 1760$.

(b) Use Lemma 3.5 to show that the minimal polynomial of α has degree at most 1760.

Solution.

(a) Since α satisfies a polynomial equation of degree 11, by the tower theorem, we have

$$[L : \mathbb{Q}] \leq 2 \cdot 2 \cdot 4 \cdot 2 \cdot 5 \cdot 11 = 1760.$$

(b) Since $\alpha \in L$, by Lemma 3.5, the degree of the minimal polynomial of α over $\mathbb{Q}$ divides $[L : \mathbb{Q}] = 1760$, so it follows that the degree of the minimal polynomial is at most 1760. □

Example 3.38 (Trinity College Dublin Michaelmas 2013)**.** Use the tower theorem to prove that the set of all algebraic numbers is a subfield of $\mathbb{C}$.

Solution. Note that $z \in \mathbb{C}$ is algebraic if and only if it is algebraic over $\mathbb{Q}$. It is clear that for $w, z \in \mathbb{C}$, $\mathbb{Q}(z) \subseteq \mathbb{Q}(z)(w)$ is a finite field extension. Recall the definition of such an example of a field extension. On the left, for the field $\mathbb{Q}(z)(w)$, This can be thought of as the set of numbers of the form $a + bw$, where $a, b \in \mathbb{Q}(z)$.

Note that $\mathbb{Q}(z,w)=\mathbb{Q}(z)(w)$. Now, recall the tower theorem which states that

$$\text{for field extensions } E\subseteq F \text{ and } F\subseteq G \quad \text{we have} \quad [G:E]=[G:F][F:E]$$

Also, recall that $\mathbb{Q}(z)\subseteq\mathbb{Q}(z)(w)=\mathbb{Q}(z,w)$ and note that $\mathbb{Q}\subset\mathbb{Q}(z)$. By the tower theorem, $\mathbb{Q}\subseteq\mathbb{Q}(z,w)$ is a finite field extension. All that is left is to verify that $z+w$, $z-w$, zw and zw^{-1} are algebraic numbers in order to show that the set of all algebraic numbers $\mathbb{Q}(z,w)$ is a subfield of $\mathbb{C}$. This is obvious. □

In addition to the notion of an algebraic number in $\mathbb{C}$, one can also define algebraic integers!

Definition 3.12 (algebraic integer). An algebraic integer is a complex number that is a root of a monic polynomial with integer coefficients.

Example 3.39. $\sqrt{2}$ and $\omega=\left(-1+i\sqrt{3}\right)/2$ are algebraic integers since they are roots of x^2-2 and x^2+x+1 respectively.

Algebraic integers play an important role in Algebraic Number Theory. For example, Euler proved Fermat's last theorem for $n=3$ by writing $x^3+y^3=z^3$ as

$$x^3=z^3-y^3=(z-y)(z-\omega y)\left(z-\omega^2y\right)$$

and using unique factorisation in the ring of algebraic integers $\mathbb{Z}[\omega]$. The interested reader is recommended to refer to Daniel Marcus' book on 'Number Fields' or ' Algebraic Number Theory and Fermat's Last Theorem' by David Tall and Ian Stewart.

Example 3.40 (Cox p. 98 Question 3). In Definition 3.12, we defined an algebraic integer to be a complex number $\alpha\in\mathbb{C}$ that is a root of a monic polynomial in $\mathbb{Z}[x]$.

(a) Prove that $\alpha\in\mathbb{C}$ is an algebraic integer if and only if α is an algebraic number whose minimal polynomial over $\mathbb{Q}$ has integer coefficients.

(b) Show that $\omega/2$ is not an algebraic integer, where $\omega=\left(-1+i\sqrt{3}\right)/2$.

Solution.

(a) For the forward direction, suppose $\alpha\in\mathbb{C}$ is an algebraic integer. Say the monic polynomial is p, so $p(\alpha)=0$, where $p\in\mathbb{Z}[x]$ is monic. Write $P=\mathbb{Q}[x]$ as the minimal polynomial of α over $\mathbb{Q}$. Then, $P\mid p$ in $\mathbb{Q}[x]$, i.e. there exists $q\in\mathbb{Q}[x]$ such that $p=Pq$.

So, there exists $\delta\in\mathbb{A}$ such that $\tilde{P}=\delta P,\tilde{q}=\delta^{-1}q\in\mathbb{Z}[x]$. So, $p=\tilde{P}\tilde{q}$, where $\tilde{P},\tilde{q}\in\mathbb{Z}[x]$. Since p is monic, then $\tilde{P},\tilde{q}$ are also monic. It follows that $P=\tilde{P}$, with $P\in\mathbb{Z}[x]$.

The reverse direction is straightforward. If the minimal polynomial P of α over $\mathbb{Q}$ has integer coefficients, then P is an example of a monic polynomial such that $P(\alpha)=0$, so α is an algebraic integer.

(b) We have

$$\frac{\omega}{2} = \frac{1}{2}e^{2\pi i/3}$$

$\omega/2$ is a root of $z^3 - 1/8 = 0$, but this polynomial is not monic. As such, $\omega/2$ is not an algebraic integer. □

4. Normal and Separable Extensions

4.1. *Splitting Fields*

For any field F, we know that if $f(x) \in F[x]$, then there exists a field extension L of F such that $f(x)$ splits completely. This motivates the definition of a splitting field (Definition 4.1).

Definition 4.1 (splitting field)**.** Let $f(x) \in F[x]$ with $\deg(f) = n > 0$. A field extension L of F is a splitting field of $f(x)$ over F if the following hold:

(i) $f(x) = c(x-\alpha_1)\ldots(x-\alpha_n)$ where $c \in F$ and $a_i \in L$ for all $1 \le i \le n$

(ii) $L = F(\alpha_1, \ldots, \alpha_n)$

Note that the field extension L in Definition 4.1 is the smallest extension over which a polynomial splits completely. Recall that the existence of splitting fields follows due to Kronecker's theorem (Theorem 3.2), which mentions if $f \in F[x]$ splits completely as $f = c(x-\alpha_1)\ldots(x-\alpha_n)$ in $L[x]$, then $F(\alpha_1, \ldots, \alpha_n)$ is a splitting field of f over F.

We first give some examples of splitting fields.

Example 4.1. First, note that

$$\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) = \mathbb{Q}\left(\pm\sqrt{2},\pm\sqrt{3}\right).$$

This field is a splitting field of $\left(x^2-2\right)\left(x^2-3\right)$ over $\mathbb{Q}$ as this polynomial factorises as linear factors, i.e.

$$\left(x^2-2\right)\left(x^2-3\right) = \left(x+\sqrt{2}\right)\left(x-\sqrt{2}\right)\left(x+\sqrt{3}\right)\left(x-\sqrt{3}\right)$$

with the first two terms being obvious elements of $\mathbb{Q}\left(\sqrt{2}\right)$ and the other two being elements of $\mathbb{Q}\left(\sqrt{3}\right)$. By using the fact that $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt{3}\right)$.

Example 4.2. Recall that

$$\mathbb{Q}\left(\sqrt[4]{2},-\sqrt[4]{2},-\sqrt[4]{2},-i\sqrt[4]{2}\right) = \mathbb{Q}\left(i,\sqrt[4]{2}\right).$$

So, $\mathbb{Q}\left(i,\sqrt[4]{2}\right)$ is a splitting field of x^4-2 over $\mathbb{Q}$.

Example 4.3 (Cox p. 106 Question 1)**.** Let $\omega = e^{2\pi i/3}$. Then, a splitting field of x^3-2 over $\mathbb{Q}$ is $\mathbb{Q}\left(\omega,\sqrt[3]{2}\right)$. To see why, note that

$$\text{the solutions to } x^3-2=0 \quad \text{are} \quad x = \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2.$$

As such,

$$x^3-2 = \left(x-\sqrt[3]{2}\right)\left(x-\sqrt[3]{2}\omega\right)\left(x-\sqrt[3]{2}\omega^2\right).$$

Each of the roots $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ is contained in the field $\mathbb{Q}\left(\omega,\sqrt[3]{2}\right)$. So, it follows that $\mathbb{Q}\left(\omega,\sqrt[3]{2}\right)$ is indeed a splitting field of x^3-2 over $\mathbb{Q}$.

We note that a splitting field of $f \in F[x]$ depends on both the polynomial f and the field F. For instance,

$$\begin{aligned} &\text{a splitting field of } x^2+1 \text{ over } \mathbb{Q} && \text{is } \mathbb{Q}(i) \\ &\text{a splitting field of } x^2+1 \text{ over } \mathbb{R} && \text{is } \mathbb{C} \\ &\text{a splitting field of } x^2+1 \text{ over } \mathbb{C} && \text{is } \mathbb{C} \end{aligned}$$

Well, to see why, consider the polynomial $f(x) = x^2+1 \in \mathbb{Q}[x]$. Since $x^2+1 = (x+i)(x-i)$, then f splits over $\mathbb{C}$, but a splitting field over $\mathbb{Q}$ is $\mathbb{Q}(i) = \{a+bi : a,b \in \mathbb{Q}\}$.

Likewise, $x^2-2 \in \mathbb{Q}[x]$ splits over $\mathbb{R}$ but a splitting field over $\mathbb{Q}$ is $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a+b\sqrt{2} : a,b \in \mathbb{Q}\right\}$.

There is a useful analogy between the definition of a splitting field and the definition of an irreducible polynomial. Just as it makes no sense to say that '$f(x)$ is irreducible', it then makes no sense to say 'L is a splitting field for $f(x)$'. In each case, the underlying field must be specified, i.e. one must say '$f(x)$ is irreducible over F' and 'L is a splitting field for $f(x)$ over F'.

Since the roots of a non-constant polynomial $f \in F[x]$ are algebraic over F, then by Theorem 3.11, a splitting field of f over F is always a finite extension of F. In fact, the degree of this extension is bounded by $n!$ as shown in Theorem 4.1.

Theorem 4.1 (bounding degree of field extension)**.** Le $f \in F[x]$ be a polynomial of degree $n > 0$, and let L be a splitting field of f over F. Then, $[L:F] \leq n!$.

We will see a couple of examples of Theorem 4.1 having equality and inequality as shown in Examples 4.4 and 4.5 respectively.

Example 4.4. Recall that

$$\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) \quad \text{is a splitting field of } \left(x^2-2\right)\left(x^2-3\right) \text{ over } \mathbb{Q}$$

and the degree of this field extension is 4. The degree of the minimal polynomial obtained is 4 as well but $4 < 4!$.

Example 4.5. Recall that

$$\mathbb{Q}\left(\omega,\sqrt[3]{2}\right) \quad \text{is a splitting field of } x^3-2 \text{ over } \mathbb{Q}$$

and the degree of this field extension is $2 \cdot 3 = 6$ by the tower theorem (Theorem 3.9). Also, the degree of the minimal polynomial obtained is 3. One checks that the formula in Theorem 4.1 holds as $6 = 3!$.

We then discuss the uniqueness of splitting fields. We will see that they are unique up to isomorphism. A given polynomial $f \in F[x]$ will have many distinct splitting fields. For example,

$$\mathbb{Q}\left(\sqrt{2}\right) \text{ and } \mathbb{Q}[t]/\left(t^2-2\right) \quad \text{are splitting fields of } x^2-2 \text{ over } \mathbb{Q}.$$

Although these fields are not the same, they are isomorphic. In fact, we can prove such a result for all polynomials, so we shall establish a more general fact. Say we have an isomorphism of fields $\varphi : F_1 \cong F_2$ and let $f_1 \in F_1[x]$ be a polynomial of degree $n > 0$. Applying φ to the coefficients of f_1 yields a polynomial $f_2 \in F_2[x]$.

Let L_i be a splitting field of f_i over F_i for $i = 1, 2$. Then, this yields the following diagram:

$$\begin{tikzcd}
L_1 \arrow[r, "\overline{\varphi}"] & L_2 \\
F_1 \arrow[u, phantom, "\cup\!\mid"] \arrow[r, "\varphi"] & F_2 \arrow[u, phantom, "\cup\!\mid"]
\end{tikzcd}$$

Although the splitting fields L_1 and L_2 might be constructed using different ways, they are always isomorphic as shown in Theorem 4.2.

Theorem 4.2. Suppose $f_1 \in F_1[x]$ and there exists an isomorphism $\varphi : F_1 \cong F_2$. Then,

$$\text{there exists an isomorphism } \overline{\varphi} : L_1 \cong L_2 \quad \text{such that} \quad \varphi = \overline{\varphi}|_{F_1}.$$

When applied to the identity map $1_F : F \to F$ and $f \in F[x]$, Theorem 4.2 yields the following corollary on a uniqueness result for splitting fields.

Corollary 4.1. Suppose L_1, L_2 are splitting fields of $f \in F[x]$. Then,

$$\text{there exists} \quad \text{an isomorphism } L_1 \cong L_2 \text{ that is the identity on } F.$$

As such, we are now in position to discuss the unique splitting field of $f \in F[x]$, provided that we remember that splitting fields are unique up to isomorphism.

Proposition 4.1. Let L be a splitting field of a polynomial in $F[x]$, and suppose $h \in F[x]$ is irreducible and has roots $\alpha, \beta \in L$. Then,

$$\text{there exists a field isomorphism } \sigma : L \to L \quad \text{that is} \quad \text{the identity on } F \text{ and } \sigma(\alpha) = \beta.$$

Example 4.6. Again, recall that $L = \mathbb{Q}\left(\sqrt{2}\right)$ is the splitting field of $x^2 - 2$ over $\mathbb{Q}$. This polynomial is irreducible over $\mathbb{Q}$ and has roots $\pm\sqrt{2} \in L$. By Proposition 4.1,

$$\text{there exists an isomorphism } \sigma : L \to L \quad \text{such that} \quad \sigma\left(\sqrt{2}\right) = -\sqrt{2}.$$

Of course, the *roles* of $\sqrt{2}$ and $-\sqrt{2}$ can be swapped, i.e. we can also say that there exists an isomorphism $\sigma : L \to L$ such that $\sigma\left(-\sqrt{2}\right) = \sqrt{2}$. We will see that using Proposition 4.1 is closely tied to the definition of a Galois group (Definition 5.1), i.e.

$$\text{an isomorphism } \sigma : L \cong L \quad \text{that is} \quad \text{the identity on } F \subseteq L$$

is an element of the Galois group $\operatorname{Gal}(L/F)$. In due course, one would see that we can construct elements of the Galois group $\operatorname{Gal}(L/F)$ when L is a splitting field over F.

Example 4.7 (Cox p. 106 Question 13)**.** Let $L = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. Use Proposition 4.1 to prove that there is

$$\text{an isomorphism } \sigma : L \cong L \quad \text{such that} \quad \sigma\left(\sqrt{2}\right) = \sqrt{2} \text{ and } \sigma\left(\sqrt{3}\right) = -\sqrt{3}.$$

Solution. As a motivation, we observe that $\sqrt{2}$ is fixed under σ so we should consider the extension $\mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)^{\dagger}$. We first claim that $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ is the splitting field of $x^2 - 3$ over $\mathbb{Q}\left(\sqrt{2}\right)$. This is easy to see because $x^2 - 3$ is irreducible over $\mathbb{Q}\left(\sqrt{2}\right)$. Hence, by Proposition 4.1,

$$\text{there exists a field isomorphism } \sigma : L \to L \quad \text{that is the identity on } \mathbb{Q}\left(\sqrt{2}\right) \text{ and } \sigma\left(\sqrt{3}\right) = -\sqrt{3}.$$

Here, we set $\alpha = \sqrt{3}$ and $\beta = -\sqrt{3}$. As σ is the identity on $\mathbb{Q}\left(\sqrt{2}\right)$, it follows that $\sigma\left(\sqrt{2}\right) = \sqrt{2}$. □

4.2. *Normal Extensions*

Proposition 4.2. Let L be the splitting field of $f \in F[x]$, and let $g \in F[x]$ be irreducible. If g has one root in L, then g splits completely over L.

Example 4.8. We justify that $\mathbb{Q}\left(\sqrt[3]{2}\right)$ is not the splitting field of any polynomial in $\mathbb{Q}[x]$. To see why, recall that $x^3 - 2$ is irreducible over $\mathbb{Q}$ and has a root in $\mathbb{Q}\left(\sqrt[3]{2}\right)$. If this field were a splitting field, then by Proposition 4.2, $x^3 - 2$ must split completely over $\mathbb{Q}\left(\sqrt[3]{2}\right)$. However, this is impossible since $\mathbb{Q}\left(\sqrt[3]{2}\right) \subseteq \mathbb{R}$ does not contain the other two complex roots of $x^3 - 2$, namely $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$.

Definition 4.2 (normal extension)**.** An algebraic extension $F \subseteq L$ is normal if every irreducible polynomial in $F[x]$ that has a root in L splits completely over L.

Example 4.9 (Cox p. 109 Question 1)**.** Prove that $\mathbb{Q}\left(\sqrt[4]{2}\right)$ is not the splitting field of any polynomial in $\mathbb{Q}[x]$.

Solution. Note that

$$\left(x + \sqrt[4]{2}\right)\left(x - \sqrt[4]{2}\right) = x^2 - \sqrt{2}.$$

[†] I do not wish to make this part of the main notes but this is intended for readers who have already read the next chapter on 'Galois groups'. We mentioned when motivating the solution to this question that $\sqrt{2}$ is fixed under σ, but we purposely did not mention that $\sigma\left(\sqrt{3}\right) = -\sqrt{3}$, although this does not affect anything. One sees that this is an automorphism of $L = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ since $\sigma^2\left(\sqrt{3}\right) = \sqrt{3}$. We will revisit this idea in Example 5.7

In order to obtain some polynomial in $\mathbb{Q}[x]$, the natural thing to do is to multiply $x^2-\sqrt{2}$ by its conjugate $x^2+\sqrt{2}$, which in turns yields x^4-2. Note that x^4-2 is irreducible over $\mathbb{Q}$ by Eisenstein's criterion (Theorem 3.7). Moreover, x^4-2 is the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ but it has roots $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$.

However, the roots $i\sqrt[4]{2}, -i\sqrt[4]{2}$ are purely imaginary, so it is not contained in $\mathbb{Q}\left(\sqrt[4]{2}\right) \subseteq \mathbb{R}$. Hence, $\mathbb{Q}\left(\sqrt[4]{2}\right)$ is not a normal extension of $\mathbb{Q}$, and the result follows. □

Example 4.10 (Cox p. 109 Question 2)**.** Prove that an algebraic extension $F \subseteq L$ is normal if and only if

$$\text{for every } \alpha \in L \quad \text{the minimal polynomial of } \alpha \text{ over } F \text{ splits completely over } L.$$

Solution. We first prove the forward direction. Suppose $F \subseteq L$ is normal. Its minimal polynomial of α, denoted by $f \in F[x]$, is irreducible over F, so by definition, the minimal polynomial splits completely over L.

Conversely, let g be some irreducible polynomial in $F[x]$ that has a root $\alpha \in L$, so g is the minimal polynomial of α over L. Hence, g splits completely over L, making $F \subseteq L$ a normal extension. □

Theorem 4.3. Suppose $F \subseteq L$. Then,

$$L \text{ is the splitting field of some } f \in F[x] \quad \text{if and only if} \quad F \subseteq L \text{ is normal and finite.}$$

Example 4.11 (Cox p. 109 Question 3)**.** Determine whether the following extensions are normal. Justify your answers.

(a) $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ where $\zeta_n = e^{2\pi i/n}$

(b) $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right)$

(c) $F = \mathbb{F}_3(t) \subseteq F(\alpha)$, where t is a variable and α is a root of x^3-t in a splitting field

Solution.

(a) Consider

$$\zeta_n^k = e^{2k\pi i/n} \quad \text{where } 0 \leq k \leq n-1.$$

It follows that $\zeta_n^k \in \mathbb{Q}(\zeta_n)$, so $\mathbb{Q}(\zeta_n)$ is the splitting field of x^n-1 over $\mathbb{Q}$. By Theorem 4.3, $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ is normal.

(b) The minimal polynomial of $\mathbb{Q}\left(\sqrt[3]{2}\right)$ over $\mathbb{Q}$ is x^3-2, which is irreducible over $\mathbb{Q}$. However, this polynomial does not split completely over $\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right)$ since the other roots are complex. By Definition 4.2, $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right)$ is not a normal extension.

(c) Since $\operatorname{char}(F) = 3$, then

$$x^3 - t = (x-\alpha)^3 \quad \text{where } \alpha \in F(\alpha).$$

Since this polynomial splits into linear factors over $F(\alpha)$, it follows that $F(\alpha)$ is a splitting field for x^3-t over $\mathbb{F}_3(t)$. By Theorem 4.3, $\mathbb{F}_3(t) \subseteq F(\alpha)$ is a normal extension. □

Example 4.12 (Cox p. 109 Question 4)**.** Give an example of a normal extension of $\mathbb{Q}$ that is not finite.

Solution. We will show that

$$\mathbb{Q} \subseteq \mathbb{A} \text{ is a normal extension} \quad \text{but} \quad \text{infinite.}$$

Recall that $\mathbb{A}$ is an algebraically closed field by Theorem 3.10. Say $f \in \mathbb{Q}[x]$ is an irreducible polynomial over $\mathbb{Q}$, so $f \in \mathbb{A}[x]$. Recall the definition of an algebraically closed field (Definition 3.5) which mentions that f must split completely over $\mathbb{A}$. As such, $\mathbb{Q} \subseteq \mathbb{A}$ is a normal extension.

However, in Example 3.33, we used the tower theorem to deduce that $[\mathbb{A} : \mathbb{Q}]$ is infinite, so $\mathbb{Q} \subseteq \mathbb{A}$ is not a finite extension. □

4.3. *Separable Extensions*

Given a non-constant polynomial $f \in F[x]$ with splitting field $F \subseteq L$, we can write

$$f = a_0 \prod_{i=1}^{n} (x-\alpha_i) \quad \text{where } a_0 \in F \text{ and } \alpha_1, \ldots, \alpha_n \in L.$$

It is important to realise that $\alpha_1, \ldots, \alpha_n$ are not always distinct. This is quite obvious. For example,

$$f(x) = x^2 - 2x + 1 \in \mathbb{Q}[x] \quad \text{has } \alpha_1 = \alpha_2 = 1.$$

Here, we will study special polynomials for which the roots are all different. Such polynomials are given a special name — separable.

Definition 4.3. Let $f \in F[x]$ be a non-constant polynomial such that

$$f = a_0 \prod_{i=1}^{n} (x-\alpha_i) \quad \text{where } a_0 \in F \text{ and } \alpha_1, \ldots, \alpha_n \in L.$$

Then, we can write this equation as

$$f = a_0 \prod_{i=1}^{n} (x-\beta_i)^{m_i} \quad \text{where } a_0 \in F \text{ and } \beta_1, \ldots, \beta_r \in L \text{ are distinct and } m_1, \ldots, m_r \geq 1.$$

We say that m_i is the multiplicity of β_i. β_i is a simple root if $m_i = 1$ and a multiple root if $m_i > 1$.

We now define what a separable polynomial is.

Definition 4.4 (separable polynomial)**.** A polynomial $f \in F[x]$ is separable if it is non-constant and its roots in a splitting field are all simple. In other words, f is separable if it has distinct roots.

Note that the definition of a separable polynomial is independent of the splitting field used since all splitting fields of f over F are unique up to isomorphism.

In order to study separability, we will use a tool that was discussed at the early stage of the course — the discriminant Δ! In particular, we shall consider the discriminant $\Delta(f) \in F$ of a monic polynomial $f \in F[x]$. Recall that if $\deg(f) > 1$, then

$$\Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2 \quad \text{when} \quad f = \prod_{i=1}^{n} (x - \alpha_i).$$

Another tool that we will need is the formal derivative, which for a polynomial $g = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + a_n x^n \in F[x]$ is defined to be

$$g' = a_1 + \ldots + (n-1)a_{n-1}x^{n-2} + na_n x^{n-1}.$$

The operation $g \mapsto g'$ enjoys the usual properties from Calculus, including

$$(ag + bh)' = ag' + bh' \quad \text{and} \quad (gh)' = gh' + g'h$$

for $g, h \in F[x]$ and $a, b \in F$. On page 117 of Cox's textbook, Question 1 asks the reader to prove these two results, which are rather trivial since they enjoy nice properties of derivatives of polynomials. We now see that separability, the discriminant, and the formal derivative are related as follows:

Proposition 4.3. If $f \in F[x]$ is monic and non-constant, then the following are equivalent:

(i) f is separable

(ii) $\Delta(f) \neq 0$

(iii) f and f' are relatively prime in $F[x]$, i.e. $\gcd(f, f') = 1$

Definition 4.5 (separable element and separable extension)**.** Let $F \subseteq L$ be an algebraic extension.

(i) $\alpha \in L$ is separable over F if its minimal polynomial over F is separable

(ii) $F \subseteq L$ is a separable extension if every $\alpha \in L$ is separable over F

We can interpret the separability of a polynomial in terms of its irreducible factors as follows:

Lemma 4.1. A non-constant polynomial $f \in F[x]$ is separable if and only if it is a product of irreducible polynomials, each of which is separable and no two of which are multiples of each other.

Lemma 4.2. Let $f \in F[x]$ be an irreducible polynomial of degree n. Then, f is separable if either

$$\operatorname{char}(F) = 0 \quad \text{or} \quad \operatorname{char}(F) = p > 0 \text{ and } p \text{ does not divide } n.$$

Here, p is prime.

Example 4.13. Consider $f = x^n - 1 \in F[x]$, where $n > 0$. By Proposition 4.3,

$$f \text{ is separable} \quad \text{if and only if} \quad \gcd\left(f, f'\right) = 1.$$

The gcd claim can be put more explicit, i.e. noting that $f' = nx^{n-1}$, we must have $\gcd\left(x^n, nx^{n-1}\right) = 1$.

If $n \neq 0$ in F, then the only irreducible factor of f' is x, which does not divide f. Hence, $\gcd(f, f') = 1$. On the other hand, if $n = 0$ in F, then $f' = 0$. It follows that $f \mid f'$, i.e. $\gcd(f, f') > 1$. It follows that $x^n - 1 \in F[x]$ fails to be separable if and only if $\operatorname{char}(F) = p$ and p divides n.

Proposition 4.4. If $\operatorname{char}(F) = 0$, then the following hold:

(i) Every irreducible polynomial in $F[x]$ is separable

(ii) Every algebraic extension of F is separable

(iii) A non-constant polynomial $f \in F[x]$ is separable if and only if f is a product of irreducible polynomials, no two of which are multiples of each other

We briefly talk about the proof of **(ii)**. Let L be an algebraic extension of F, so the minimal polynomial of α over F is separable. The result follows.

In fields with characteristic 0, we can get rid of multiple roots as follows:

Proposition 4.5. Suppose $\operatorname{char}(F) = 0$, and suppose $f \in F[x]$ has the factorisation $f = cg_1^{m_1} \ldots g_l^{m_l}$, where $c \in F$, $g_i \in F[x]$ is monic and irreducible for all $1 \leq i \leq l$ and $g_1, \ldots, g_l$ are distinct. Then,

$$\frac{f}{\gcd(f, f')} = cg_1 \ldots g_l.$$

Furthermore, $g_1, \ldots, g_l$ is separable and has the same roots as f in a splitting field.

This proposition is more powerful than it seems. For example, suppose we have a polynomial $f \in F[x]$ that has multiple roots in a splitting field, say

$$f = a_0 (x - \beta_1)^{m_1} \ldots (x - \beta_r)^{m_r} \quad \text{where } a_0 \in F \text{ and } \beta_1, \ldots, \beta_r \text{ distinct and } m_l \geq 1.$$

If we ignore the multiplicities, the new obtain the separable polynomial

$$g = a_0 \prod_{i=1}^{r} (x - \beta_i) \quad \text{which has the same roots as } f.$$

There are some methods to find g but we will not discuss them.

We then discuss some properties of fields of characteristic p.

Lemma 4.3 (freshman's dream). Let F be a field of characteristic p and $\alpha,\beta\in F$. Then,

$$(\alpha+\beta)^p=\alpha^p+\beta^p \quad \text{and} \quad (\alpha-\beta)^p=\alpha^p-\beta^p.$$

These properties mentioned in Lemma 4.3 are specific instances of freshman's dream, i.e. in fields of characteristic p. The name is somewhat informal and playful, as it refers to the naïve hope that $(\alpha+\beta)^n=\alpha^n+\beta^n$ might hold for general exponents n, which is true in characteristic p for $n=p$, but not in general. For example, over the real numbers, $(x+y)^2$ and x^2+y^2 are two distinct expressions.

More formally, these equalities in Lemma 4.3 follow from the Frobenius endomorphism in fields of characteristic p. This refers to the map $x\mapsto x^p$. The key property of fields of characteristic p is that the binomial coefficients $\binom{p}{k}$ for $1\le k\le p-1$ are divisible by p, making all the intermediate terms in the binomial expansion of $(\alpha+\beta)^p$ and $(\alpha-\beta)^p$ vanish modulo p. In fact, this is precisely a rough sketch of the proof of Lemma 4.3.

Perhaps covered in MA3201, a ring homomorphism is a special type of endomorphism. As $(\alpha\beta)^p=\alpha^p\beta^p$, it follows that the map $\alpha\mapsto\alpha^p$ is a ring homomorphism over any field F of characteristic p (the weaker statement as mentioned is the Frobenius endomorphism but we usually refer to it as mentioned or the Frobenius homomorphism interchangeably).

Example 4.14 (Cox p. 117 Question 3). Let F be a field of characteristic p. The n^{th} roots of unity are defined to be

$$\text{the roots of } x^n-1 \quad \text{in} \quad \text{the splitting field } F\subseteq L \text{ of } x^n-1.$$

(a) If p does not divide n, show that there are n distinct n^{th} roots of unity in L.

(b) Show that there is only one p^{th} root of unity, namely $1\in F$.

Solution.

(a) Here, we take $n\ge 1$. As $f=x^n-1$, then $f'=nx^{n-1}$. Suppose p does not divide n, then $n\neq 0$ in the field F of characteristic p. Hence, n is a unit in $F[x]$.

It suffices to show that f is a separable polynomial, for which it follows that the n roots of f in its splitting field, which are the n^{th} roots of unity, are distinct. By Proposition 4.3, it suffices to show that $\gcd(f,f')=1$ in $F[x]$.

We have

$$x\left(nx^{n-1}\right)-n\left(x^n-1\right)=xf'-nf.$$

By the converse of Bézout's lemma, it follows that $\gcd(f,f')=1$.

(b) By freshman's dream (Lemma 4.3), since $\operatorname{char}(F)=p$, then $x^p-1=(x-1)^p$. As such, the only p^{th} root of unity is 1.

Example 4.15. Let $F = k(t)$, where k is a field of characteristic p and t is a variable. We will prove that

$$f = x^p - t \in F[x] \quad \text{is} \quad \text{non-separable and irreducible over } F.$$

To see why, note that f has no roots in F by *a long and painful argument* in Example 3.22. Since p is prime, by Proposition 3.3, f is irreducible over F. Also, if $\alpha \in L$ is a root of f in its splitting field L, then $\alpha^p = t$. By freshman's dream (Lemma 4.3), we have

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

Hence, f does not have distinct roots in its splitting field f. So, f is not a separable polynomial.

Example 4.16. Let $\mathbb{F}_2$ be the field of two elements. Then, $f = x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible since it has no roots in $\mathbb{F}_2$. This is easy to check as $f(0) = f(1) = 1$. Since $f' = 2x + 1 = 1$, then $\gcd(f, f') = 1$. By Proposition 4.3, it follows that f is a separable polynomial.

We then give some conditions that imply separability.

Theorem 4.4. Here are some conditions that imply separability.

(i) If $L = F(\alpha_1, \ldots, \alpha_n)$, where each α_i is separable over F, then $F \subseteq L$ is separable

(ii) If $F \subseteq L$ is the splitting field of a separable polynomial, then $F \subseteq L$ is separable

(iii) If $F \subseteq K$ and $K \subseteq L$ are separable extensions, then $F \subseteq L$ is separable

We shall discuss the converse of **(iii)** of Theorem 4.4.

Example 4.17 (Cox p. 118 Question 14)**.** Let $F \subseteq K \subseteq L$ be field extensions, and assume that L is separable over F. Prove that

$$F \subseteq K \quad \text{and} \quad K \subseteq L \quad \text{are separable extensions.}$$

Solution. We have every element of L being separable over F. So, every element of K is separable over F, making $F \subseteq K$ a separable extension.

Next, let $\alpha \in L$. As α is separable over F, then its minimal polynomial $f \in F[x]$ is separable. In turn, f only has simple roots in a splitting field F' of f over L. Since $f(\alpha) = 0$ and $f \in F[x] \subseteq K[x]$, it follows that the minimal polynomial f_K of α over K divides f.

As such, the order of the multiplicity of a root of f_K is at most the order of the multiplicity of this root in f. Thus, all roots of f_K in the splitting field F' are simple. So, α is separable over K. It follows that $K \subseteq L$ is separable. □

Example 4.18 (Cox p. 118 Question 9)**.** Let F be a field of characteristic p and consider $f(x) = x^p - a \in F[x]$. Assume that

$$f(x) \text{ has no root in } F \quad \text{so that} \quad f(x) \text{ is irreducible over } F.$$

Let α be a root of $f(x)$ in some extension of F.

(a) Show that $F(\alpha)$ is the splitting field of $f(x)$ and $[F(\alpha):F]=p$.

(b) Let $\beta \in F(\alpha)$ with $\beta \notin F$. Show that $\beta^p \in F$.

(c) Use **(a)** and **(b)** to show that the minimal polynomial of β over F is $x^p-\beta^p$.

(d) Conclude that $F(\alpha)$ is purely inseparable. That is to say, every element in $F(\alpha)$ but not in F is not separable over F.

Solution.

(a) We see that $f(x)=x^p-\alpha=(x-\alpha)^p$ has only one root α, where the second equality follows from $\operatorname{char}(F)=p$. The splitting field of $f(x)$ over F is thus $F(\alpha)$. Since $f(x)$ is the minimal polynomial of α over F, then $[F(\alpha):F]=\deg(f)=p$.

(b) We have $\beta \in F(\alpha)\backslash F$. There exists a polynomial $p(x)=\sum a_i x^i \in F[x]$ such that

$$\beta = p(\alpha)=\sum a_i\alpha^i.$$

By the binomial theorem,

$$\beta^p=\sum a_i^p\alpha^{pi}\in F.$$

The inclusion follows as we can repeatedly apply $\alpha^p=a$.

(c) It is clear that β is a root of $x^p-\beta^p\in F[x]$. This is equivalent to $(x-\beta)^p$. As $\beta\notin F$, then $x^p-\beta^p$ has no root in F, implying that $x^p-\beta^p$ is irreducible over F. The result follows.

(d) From **(c)**, any $\beta\in F(\alpha)\backslash F$ has a minimal polynomial of the form $x^p-\beta^p=(x-\beta)^p$. This polynomial consists of repeated roots — specifically, all roots are identical. So, β is not separable over F. □

Definition 4.6 (Artin-Schreier polynomial)**.** Let F be a field of characteristic p, where p is prime. For $\alpha\in F$, the polynomial

$$x^p-x-\alpha \quad \text{is called an Artin-Schreier polynomial.}$$

Example 4.19 (Cox p. 119 Question 16)**.** Let F have characteristic p and consider $f=x^p-x+a\in F[x]$.

(a) Show that f is separable.

(b) Let α be a root of f in some extension of F. Show that $\alpha+1$ is also a root.

(c) Use **(b)** to show that f splits completely over $F(\alpha)$.

(d) Use **(a)** of Theorem 4.4, which states that if

$$L=F(\alpha_1,\ldots,\alpha_n)\text{ where }\alpha_1,\ldots,\alpha_n\text{ are separable over }F\quad\text{then}\quad F\subseteq L\text{ is separable,}$$

to show that

$$F\subseteq F(\alpha)\quad\text{is}\quad\text{separable and normal.}$$

Solution.

(a) We have $f' = px^{p-1} - 1$. Using **(i)** and **(iii)** of Proposition 4.3 on equivalent conditions for a polynomial $f \in F[x]$ to be separable, it suffices to prove that

$$\gcd\left(x^p - x + a, px^{p-1} - 1\right) = 1.$$

In characteristic p,

$$px^{p-1} - 1 \equiv -1 \pmod{p}.$$

Since $\gcd(x^p - x + a, -1) = 1$ by definition, the result follows.

(b) Let $\widetilde{F}$ be an extension of F. Consider

$$\alpha^p - \alpha + a = 0 \quad \text{where } \alpha \in \widetilde{F}.$$

Then,

$$\begin{aligned}(\alpha+1)^p - (\alpha+1) + a &= \alpha^p + 1 - \alpha - 1 + a \quad \text{by Freshman's dream (Lemma 4.3)}\\ &= \alpha^p - \alpha + a = 0\end{aligned}$$

so $\alpha + 1$ is also a root of f in $\widetilde{F}[x]$.

(c) By **(b)**, we see that $\alpha+2, \ldots, \alpha+p-1$ are also roots of $f \in F[x]$. Together with α and $\alpha+1$, these roots are distinct since $0, 1, \ldots, p-1$ are the p distinct elements of the prime subfield of F, which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. As such, f splits completely over $F(\alpha)$.

(d) One sees that

$$F(\alpha) = F(\alpha, \alpha+1, \ldots, \alpha+p-1)$$

so $F(\alpha)$ is the splitting field of f. Since the Artin-Schreier polynomial $f = x^p - x + a$ is irreducible over F, then $F \subseteq F(\alpha)$ is a normal extension by Definition 4.2.

Next, we prove that $F \subseteq F(\alpha)$ is a separable extension. By **(a)**, f is separable so the minimal polynomial of α over F divides f, which has simple roots by **(i)** of Definition 4.5. As such, the minimal polynomial also has simple roots. Since each $\alpha + k$ is separable over F for $0 \le k \le p-1$, by **(a)** of Theorem 4.3, $F \subseteq F(\alpha)$ is a separable extension. □

4.4. *Primitive Element Theorem*

Of the extension fields $F \subseteq L$ studied so far, the nicest case is when $L = F(\alpha)$ for some $\alpha \in L$. When this happens, we say that α is a primitive element of $F \subseteq L$. Here, we will show that many but not all finite extensions have primitive elements.

Theorem 4.5 (primitive element theorem). Let $F \subseteq L = F(\alpha_1, \ldots, \alpha_n)$ be a finite extension, where each α_i is separable over F. Then, there exists $\alpha \in L$ separable over F such that $L = F(\alpha)$.

Furthermore, if F is infinite, then α can be chosen to be of the form

$$\alpha = t_1\alpha_1 + \ldots + t_n\alpha_n \quad \text{where } t_1, \ldots, t_n \in F.$$

To put it simply, the primitive element theorem (Theorem 4.5) states that every finite separable field extension is simple. By the term 'simple', we mean that the extension field is generated by a single element, for which in this case, we have $L = F(\alpha)$.

Corollary 4.2. Let $F \subseteq L$ be a finite extension. Then, the following hold:

(a) If $F \subseteq L$ is separable, then there exists $\alpha \in L$ such that $L = F(\alpha)$.

(b) If $\operatorname{char}(F) = 0$, then there exists $\alpha \in L$ such that $L = F(\alpha)$. Furthermore, if $L = F(\alpha_1, \ldots, \alpha_n)$, then α can be chosen to be of the form

$$\alpha = t_1\alpha_1 + \ldots + t_n\alpha_n \quad \text{where } t_1, \ldots, t_n \in F.$$

Corollary 4.2 tells us that all finite separable extensions have primitive elements. However, there exist extensions $F \subseteq L = F(\alpha)$ which are not separable but have a primitive element. Steinitz's theorem (Theorem 4.6) characterises all finite extensions that have primitive elements (note that this should not be confused with the Steinitz exchange lemma in Linear Algebra).

Theorem 4.6 (Steiniz's theorem). A finite extension $F \subseteq L$ has a primitive element if and only if there are only finitely many intermediate fields $F \subseteq k \subseteq L$.

Example 4.20. Consider the extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. Suppose $f = x^2 - 2$ and $g = x^2 - 3$. Then, f has roots $\beta_1 = \sqrt{2}$ and $\beta_2 = -\sqrt{2}$; g has roots $\gamma_1 = \sqrt{3}$ and $\gamma_2 = -\sqrt{3}$. We claim that

$$\alpha = \sqrt{2} + \lambda\sqrt{3} \text{ is a primitive element of } \mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \quad \text{for all } \lambda \in \mathbb{Q}\backslash\{0\}.$$

In other words, $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}(\alpha)$. Let $\alpha = \sqrt{2} + \lambda\sqrt{3}$. Then, we have

$$\left(\alpha - \sqrt{2}\right)^2 = 3\lambda^2 \quad \text{so} \quad \alpha^2 - 2\alpha\sqrt{2} + 2 = 3\lambda^2.$$

It follows that $\sqrt{2}$ and $\sqrt{3}$ can be expressed in terms of α. As such, $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$.

Not all finite extensions have primitive elements. As shown in **(a)** of Corollary 4.2, such an extension cannot have characteristic 0. We give an example in characteristic p in Example 4.23, but before that, we use some preliminary results obtained in Example 4.21, which was left as an exercise problem in Cox's book.

Example 4.21 (Cox p. 123 Question 4). In the extension $F \subseteq L$ of Example 4.23, we have $F = k(t,u)$, where k has characteristic p and L is the splitting field of $(x^p - t)(x^p - u) \in F[x]$. We also have $\alpha, \beta \in L$ satisfying $\alpha^p = t$ and $\beta^p = u$. Prove the following properties of $F \subseteq L$:

(a) $L = F(\alpha, \beta)$ and $[L : F] = p^2$

(b) $[F(\gamma):F]=p$ for all $\gamma \in L\backslash F$

(c) $F\subseteq L$ is purely inseparable

Solution.

(a) Since $\alpha,\beta\in L$ and because $F\subseteq L$, then $F(\alpha,\beta)\subseteq L$. We then prove the reverse inclusion. Since $\operatorname{char}(F)=p$, then

$$f=(x^p-t)(x^p-u)=(x-\alpha)^p(x-\beta)^p \quad \text{by freshman's dream}$$

and this polynomial only has the roots α and β. So, the splitting field of f over F is $F(\alpha,\beta)$. So, the reverse inclusion holds and it follows that $L=F(\alpha,\beta)$.

For the next part, it suffices to use the tower theorem (Theorem 3.9) to deduce that

$$[L:F]=[L:F(\alpha)][F(\alpha):F]=p\cdot p=p^2.$$

The polynomial x^p-u has no root in $k(t,u,\alpha)=F(\alpha)$. Since p is prime, by Proposition 3.3, $h=x^p-u$ is irreducible over $F(\alpha)$. Hence, h is the minimal polynomial of β over $F(\alpha)$. As such, by the tower theorem (Theorem 3.9), we have

$$[L:F(\alpha)]=[F(\alpha,\beta):F(\alpha)]=\deg(x^p-u)=p.$$

Also, x^p-t has no root in $F(t)$ and it is irreducible. So, x^p-t is the minimal polynomial of α over F, implying that $[F(\alpha):F]=p$. The result follows.

(b) Suppose $\gamma\in L\backslash F$. We would see in Example 4.23 that the extension $F\subseteq L$ has no primitive element, so $F(\gamma)\neq L$. As such, $F(\gamma)$ is a proper subset of L.

By the tower theorem, $d=[F(\gamma):F]$ divides $p^2=[L:F]$. If $d=1$, then $F(\gamma)=F$, where $\gamma\in F$. Also, if $d=p^2$, then $F(\gamma)=L$. In these two cases, we obtain a contradiction, so $[F(\gamma):F]=p$.

(c) By **(b)**, the degree of the minimal polynomial of γ over F is p. It suffices to prove that every $\gamma\in L\backslash F$ is inseparable. Since $\gamma^p\in F$, then γ^p is a root of $x^p-b\in F[x]$, which implies the minimal polynomial divides x^p-b. In fact, this is precisely the minimal polynomial of γ over F. As $\operatorname{char}(k)=p$, it follows that $x^p-b=(x-\gamma)^p$, i.e. the polynomial is not separable. The result follows. □

Example 4.22 (Cox p. 123 Question 5). Let $k=F_p$, the finite field of p elements and $F=k(t,u)$, where t and u are independent variables. Let α and β be roots of x^p-t and x^p-u respectively. Let $L=F(\alpha,\beta)$. Consider the intermediate fields $F\subseteq F(\alpha+\lambda\beta)\subseteq L$ as λ varies over all elements of F. Suppose $\lambda\neq\mu$ are two elements of F such that $F(\alpha+\lambda\beta)=F(\alpha+\mu\beta)$.

(a) Show that $\alpha,\beta\in F(\alpha+\lambda\beta)$.

(b) Conclude that $F(\alpha+\lambda\beta)=F(\alpha,\beta)$ and explain why this is impossible.

This example shows that there are infinitely many intermediate fields between F and L.

Solution.

(a) Since $\lambda, \mu \in F$, then $\lambda, \mu \in F(\alpha+\lambda\beta)$. Thus, $\alpha+\lambda\beta \in F(\alpha+\lambda\beta)$ and $\alpha+\mu\beta \in F(\alpha+\lambda\beta)$. Since $F(\alpha+\lambda\beta)$ is a subfield, the difference of $\alpha+\lambda\beta$ and $\alpha+\mu\beta$ is in $F(\alpha+\lambda\beta)$ too. That is, $(\lambda-\mu)\beta \in F(\alpha+\lambda\beta)$. Since $\lambda \neq \mu$, then $\beta \in F(\alpha+\lambda\beta)$. It is then clear that $\alpha \in F(\alpha+\lambda\beta)$.

(b) The inclusion $F(\alpha+\lambda\beta) \subseteq F(\alpha,\beta)$ is clear since $L = F(\alpha,\beta)$. The reverse inclusion follows by **(a)**. However, $F(\alpha,\beta)$ has no primitive element (i.e. an element that generates $F(\alpha,\beta)$) which is a contradiction. This shows that all the fields $F(\alpha+\lambda\beta)$, where λ varies all elements of F, are distinct. F being finite, there exists infinitely many intermediate fields between F and L. □

Example 4.23. Let k be a field of characteristic p and let t,u be variables. Consider the extension field

$$F = k(t,u) \subseteq L \quad \text{where} \quad L \text{ is the splitting field of } (x^p - t)(x^p - u) \in F[x].$$

Thus, there exist $\alpha, \beta \in L$ with $\alpha^p = t$ and $\beta^p = u$. As such, $L = F(\alpha,\beta)$ and $[L:F] = p^2$.

We shall prove that $F = k(t,u)$ has no primitive element. Given $\gamma \in L$, we can use $L = F(\alpha,\beta) = F[\alpha,\beta]$ to write γ as the following finite sum:

$$\gamma = \sum_{i,j} a_{ij}\alpha^i\beta^j \quad \text{where } a_{ij} \in F$$

As such,

$$\gamma^p = \left(\sum_{i,j} a_{ij}\alpha^i\beta^j\right)^p = \sum_{i,j} a_{ij}^p \alpha^{ip}\beta^{jp}$$

where the second equality follows from the fact that $\operatorname{char}(F) = p$. Since $\alpha^p = t$ and $\beta^p = u$, then

$$\gamma^p = \sum_{i,j} a_{ij}^p t^i u^j \in F.$$

Hence, γ is a root of $x^p - \gamma^p \in F[x]$, so that $[F(\gamma):F] \leq p$. Since $[L:F] = p^2$, then $L \neq F(\gamma)$ for all $\gamma \in L$. Thus, $F \subseteq L$ has no primitive element.

5. The Galois Group and The Galois Correspondence

5.1. *Galois Groups*

If L is a field, then

$$\text{an automorphism of } L \quad \text{is} \quad \text{a field isomorphism } \sigma : L \to L.$$

Definition 5.1 (Galois group)**.** Let $F \subseteq L$ be a finite extension. Then, $\text{Gal}\left(L/F\right)$ is the set

$$\left\{\sigma : L \to L : \sigma \in \text{Aut}\left(L\right) \quad \text{and} \quad \sigma\left(a\right) = a \text{ for all } a \in F\right\}.$$

What Definition 5.1 means is that $\text{Gal}\left(L/F\right)$ consists of all automorphisms of L that fix $a \in F$, i.e. the identity on F. Having said that, although Definition 5.1 is very different from the one given by Galois himself, they are actually equivalent. Galois actually only dealt with splitting fields, and for him, the Galois group consisted of certain permutations of the roots.

Proposition 5.1. $\text{Gal}\left(L/F\right)$ is a group under compositiion.

Proof. Suppose $\sigma, \tau \in \text{Gal}\left(L/F\right)$. Then,

$$\sigma, \tau : L \to L \quad \text{are automorphisms.}$$

It follows that $\sigma\tau$, which refers to the composition $\sigma \circ \tau : L \to L$, is also an automorphism. Also, if $a \in F$, then

$$\sigma \circ \tau\left(a\right) = \sigma\left(\tau\left(a\right)\right) = \sigma\left(a\right) = a \quad \text{since } \sigma, \tau \text{ are the identity on } F.$$

As such, composition gives an operation on $\text{Gal}\left(L/F\right)$ which is associative by standard properties of composition.

The identity map $1_L : L \to L$ is an isomorphism that is the identity on F. As such, 1_L is an automorphism, implying that $1_L \in \text{Gal}\left(L/F\right)$. Moroever, one checks that

$$\sigma \circ 1_L = 1_L \circ \sigma = \sigma \quad \text{for all } \sigma \in \text{Gal}\left(L/F\right)$$

so 1_L is the identity element of $\text{Gal}\left(L/F\right)$.

Lastly, any $\sigma \in \text{Gal}\left(L/F\right)$ is an automorphism, which means that its inverse $\sigma^{-1} : L \to L$ is also an automorphism. Also, if $a \in F$, then $a = \sigma\left(a\right)$, which implies $\sigma^{-1}\left(a\right) = \sigma^{-1}\left(\sigma\left(a\right)\right)$. This shows that $\sigma^{-1} \in \text{Gal}\left(L/F\right)$, i.e. existence of inverse element in group is established.

It follows that $\text{Gal}\left(L/F\right)$ is a group under composition. □

By Proposition 5.1, we know that $\mathrm{Gal}(L/F)$ is a group under composition. We call $\mathrm{Gal}(L/F)$ the Galois group of $F \subseteq L$. In order to compute Galois groups, we need to know how elements of $\mathrm{Gal}(L/F)$ behave. We begin with the following observation:

Lemma 5.1. Let $F \subseteq L$ be finite, and fix $\sigma \in \mathrm{Gal}(L/F)$. Given $h \in F[x_1, \ldots, x_n]$ and $\beta_1, \ldots, \beta_n \in L$, then

$$\sigma(h(\beta_1, \ldots, \beta_n)) = h(\sigma(\beta_1), \ldots, \sigma(\beta_n)).$$

In particular, if $h \in F[x]$ and $\beta \in L$, then $\sigma(h(\beta)) = h(\sigma(\beta))$.

Proof. This pretty much follows from Proposition 5.1, where we note that σ preserves addition and multiplication, and it is also the identity on the coefficients of h. □

Following this, there are some nice consequences concerning the Galois group.

Proposition 5.2. Let $F \subseteq L$ be a finite extension and let $\sigma \in \mathrm{Gal}(L/F)$. Then, the following hold:

(a) If $h \in F[x]$ is a non-constant polynomial with $\alpha \in L$ as a root, then $\sigma(\alpha)$ is also a root of h lying in L.

(b) If $L = F(\alpha_1, \ldots, \alpha_n)$, then σ is uniquely determined by its values on $\alpha_1, \ldots, \alpha_n$.

Corollary 5.1. Let $F \subseteq L$ be a finite extension. Then, $\mathrm{Gal}(L/F)$ is finite.

Proof. Since $F \subseteq L$ is finite, then $L = F(\alpha_1, \ldots, \alpha_n)$, where each α_i is algebraic over F. Suppose $\sigma \in \mathrm{Gal}(L/F)$. By **(b)** of Proposition 5.2, σ is uniquely determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. Let $p_i \in F[x]$ be the minimal polynomial of α_i. By **(a)** of Proposition 5.2, there are at most $\deg(p_i)$ possibilities for $\sigma(\alpha_i)$. So, $\mathrm{Gal}(L/F)$ is finite. □

Example 5.1 (Cox p. 129 Question 1). Let $L = F(\alpha_1, \ldots, \alpha_n)$, and let $p_i \in F[x]$ be a non-zero polynomial vanishing at α_i. Explain why the proof of Corollary 5.1 implies that

$$|\mathrm{Gal}(L/F)| \leq \deg(p_1) \ldots \deg(p_n).$$

Solution. In the proof, we mentioned that by **(b)** of Proposition 5.2, $\sigma \in \mathrm{Gal}(L/F)$ is uniquely determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$, where ea α_i is algebraic over F. Since $p_i(\alpha_i) = 0$, applying σ on both sides yields

$$\sigma(p_i(\alpha_i)) = \sigma(0) \quad \text{so} \quad p_i(\sigma(\alpha_i)) = 0.$$

This means that $\sigma(\alpha_i)$ is also a root of p_i. Consequently, $\sigma(\alpha_i)$ can only take values in the set of roots of p_i. As such, p_i has at most $\deg(p_i)$ roots. For each α_i, $\sigma(\alpha_i)$ can only take one of these at most $\deg(p_i)$ roots. The result follows. □

Example 5.2 (Cox p. 130 Question 5). Prove the following inequalities:

(a $\left|\text{Gal}\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3},\sqrt{5}\right)/\mathbb{Q}\right)\right| \leq 8$

(b $\left|\text{Gal}\left(\mathbb{Q}\left(\sqrt{p_1},\ldots,\sqrt{p_n}\right)/\mathbb{Q}\right)\right| \leq 2^n$, where $p_1,\ldots,p_n$ are the first n primes

In each case, one can show that these are actually equalities.

Solution.

(a) We see that $2,3,5$ are the first three primes, so we shall denote them by p_1,p_2,p_3 respectively. Note that the minimal polynomial of $\sqrt{p_i}$ over $\mathbb{Q}$ is x^2-p_i. Let the minimal polynomial be denoted by q_i. Then, $\deg(q_i)=2$. So, the order of the Galois group can be bounded above by $2^3=8$.

In fact, we proved the equality case.

(b) Very similar idea compared as **(a)**. □

Example 5.3 (Cox p. 130 Question 6). Let $L=\mathbb{Q}\left(\sqrt{6},\sqrt{10},\sqrt{15}\right)$. Show that $\text{Gal}(L/\mathbb{Q}) \leq 4$.

Solution. Note that $\sqrt{15} \in \mathbb{Q}\left(\sqrt{6},\sqrt{10}\right)$ because $\left(\sqrt{6}+\sqrt{10}\right)^2 = 16+4\sqrt{15}$. Hence, $L = \mathbb{Q}\left(\sqrt{6},\sqrt{10}\right)$ and the result follows. □

Example 5.4. Consider the extension

$$\mathbb{Q} \subseteq L = \mathbb{Q}\left(\sqrt[3]{2}\right).$$

Again, the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is x^3-2, which has roots $\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}$, where $\omega=e^{2\pi i/3}$. The last two are not real and hence, cannot lie in L.

As such, every $\sigma \in \text{Gal}(L/\mathbb{Q})$ must satisfy $\sigma\left(\sqrt[3]{2}\right)=\sqrt[3]{2}$ (recall that this Galois group must contain automorphisms of L, but more importantly, they must fix the elements in the subfield $\mathbb{Q}$). Since σ is uniquely determined by $\sigma\left(\sqrt[3]{2}\right)$, it must be the identity (note that **(b)** of Proposition 5.2 is used here). As such, $\text{Gal}(L/\mathbb{Q})=\{1_L\}$.

We now provide some examples of non-trivial Galois groups.

Example 5.5 (complex conjugation). Let

$$\tau:\mathbb{C}\to\mathbb{C} \text{ be complex conjuation,} \quad \text{i.e.} \quad \tau(z)=\overline{z} \text{ for } z\in\mathbb{C}.$$

Note that τ is a homomorphism of fields since $\mathbb{C}$ is a field. Also, τ is an automorphism because $\tau\circ\tau$ is the identity. Furthermore,

$$\text{for any } a\in\mathbb{R} \text{ we have } \tau(a)=a \quad \text{so} \quad \tau\in\text{Gal}(\mathbb{C}/\mathbb{R}).$$

As such, $\text{Gal}(\mathbb{C}/\mathbb{R})$ has at least two elements since $1_{\mathbb{C}}\in\text{Gal}(\mathbb{C}/\mathbb{R})$.

We also know that $\mathbb{C}=\mathbb{R}(i)$. Since the roots of x^2+1 are $\pm i$, by **(b)** of Proposition 5.2, every

$\sigma \in \text{Gal}(\mathbb{C}/\mathbb{R})$ is uniquely determined by $\sigma(i) = \pm i$. To be slightly more explicit, we have

$$(\sigma(i))^2 = \sigma(i) \cdot \sigma(i) = (\pm i)^2 = -1$$

for which **(b)** of Proposition 5.2 becomes more apparent. Hence, $\text{Gal}(\mathbb{C}/\mathbb{R})$ has at most two elements. We conclude that $|\text{Gal}(\mathbb{C}/\mathbb{R})| = 2$, i.e.

$$\text{Gal}(\mathbb{C}/\mathbb{R}) = \{1_{\mathbb{C}}, \tau\} \quad \text{so} \quad \text{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}.$$

Example 5.6. Recall our favourite extension $\mathbb{Q} \subseteq L = \mathbb{Q}\left(\sqrt{2}\right)$. Again, by **(b)** of Proposition 5.2,

$$\sigma \in \text{Gal}(L/\mathbb{Q}) \quad \text{is uniquely determined by} \quad \sigma\left(\sqrt{2}\right) = \pm\sqrt{2}.$$

Thus, $|\text{Gal}(L/\mathbb{Q})| \leq 2$. In fact, equality holds. We shall see why from two perspectives.

- **Perspective 1:** One notes that $\sigma\left(a + b\sqrt{2}\right) = a - b\sqrt{2}$ is an automorphism of L. This is easy to see because $\sigma^2\left(a + b\sqrt{2}\right) = a + b\sqrt{2}$.
- **Perspective 2:** $L = \mathbb{Q}\left(\sqrt{2}\right)$ is the splitting field of $x^2 - 2$ over $\mathbb{Q}$. Since $x^2 - 2$ is irreducible over $\mathbb{Q}$ and $\pm\sqrt{2} \in L$, by Proposition 4.1, there exists an automorphism of L, say σ, such that $\sigma\left(\sqrt{2}\right) = -\sqrt{2}$ and is the identity on $\mathbb{Q}$.

Example 5.7 (Cox p. 129 Question 2)**.** For the extension $\mathbb{Q} \subseteq L = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$, we see that $\sigma \in \text{Gal}(L/\mathbb{Q})$ is uniquely determined by

$$\sigma\left(\sqrt{2}\right) = \pm\sqrt{2} \text{ and } \sigma\left(\sqrt{3}\right) = \pm\sqrt{3} \quad \text{by Proposition 5.2.}$$

Again, this proposition keeps appearing! The natural question is whether all possible sign equations in the above two equations actually occur. If so, it would imply that $|\text{Gal}(L/\mathbb{Q})| = 4$.

We now address the elephant in the room, which is precisely the question taken from Cox's textbook. Consider the extension $\mathbb{Q} \subseteq L = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. In Example 4.7, we used Proposition 4.1 to construct

$$\text{an automorphsim of } L \quad \text{that} \quad \text{takes } \sqrt{3} \text{ to } -\sqrt{3} \text{ and is the identity on } \mathbb{Q}\left(\sqrt{2}\right).$$

By interchanging the roles of 2 and 3 in this construction, explain why all possible signs in $\sigma\left(\sqrt{2}\right) = \pm\sqrt{2}$ and $\sigma\left(\sqrt{3}\right) = \pm\sqrt{3}$ can occur. This shows that $|\text{Gal}(L/\mathbb{Q})| = 4$.

Solution. In Example 4.7, we considered the extension $\mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. This time, to achieve the opposite effect, we shall consider the extension $\mathbb{Q}\left(\sqrt{3}\right) \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ instead. By Proposition 4.1,

$$\text{there exists an isomorphism } \tau : L \to L \quad \text{such that} \quad \tau\left(\sqrt{3}\right) = \sqrt{3} \text{ and } \tau\left(\sqrt{2}\right) = -\sqrt{2}.$$

In other words, τ is the identity on $\mathbb{Q}\left(\sqrt{3}\right)$ and it takes $\sqrt{2}$ to $-\sqrt{2}$.

In Proposition 5.1, we know that $\text{Gal}\left(L/\mathbb{Q}\right)$ is a group under composition. So, for any $\sigma, \tau \in \text{Gal}\left(L/\mathbb{Q}\right)$, the closure property of a group is satisfied, i.e. $\sigma\tau \in \text{Gal}\left(L/\mathbb{Q}\right)$. As such, $(\sigma\tau)\left(\sqrt{2}\right) = -\sqrt{2}$ and $(\sigma\tau)\left(\sqrt{3}\right) = -\sqrt{3}$. This shows that all the aforementioned possibilities can occur, so $\left|\text{Gal}\left(L/\mathbb{Q}\right)\right| \geq 4$. Earlier, we mentioned that $\left|\text{Gal}\left(L/\mathbb{Q}\right)\right| \leq 4$, so combining these two results yields $\left|\text{Gal}\left(L/\mathbb{Q}\right)\right| = 4$.

We can list the elements of this Galois group, which are

$$\text{Gal}\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right) = \{1_L, \sigma, \tau, \sigma\tau\}.$$

To reiterate again, we have the following:

$$\begin{aligned} 1_L\left(\sqrt{2}\right) &= \sqrt{2} \quad \text{and} \quad 1_L\left(\sqrt{3}\right) = \sqrt{3} \\ \sigma\left(\sqrt{2}\right) &= \sqrt{2} \quad \text{and} \quad \sigma\left(\sqrt{3}\right) = -\sqrt{3} \\ \tau\left(\sqrt{2}\right) &= -\sqrt{2} \quad \text{and} \quad \tau\left(\sqrt{3}\right) = \sqrt{3} \\ (\sigma\tau)\left(\sqrt{2}\right) &= -\sqrt{2} \quad \text{and} \quad (\sigma\tau)\left(\sqrt{3}\right) = -\sqrt{3} \end{aligned}$$

where each of the four maps are automorphisms $L \to L$. □

Finally, we study what happens when we go to an isomorphic field.

Proposition 5.3 (conjugation by field isomorphism). Suppose $F \subseteq L_1$ and $F \subseteq L_2$ are finite extensions, and let $\varphi : L_1 \to L_2$ be an isomorphism that is the identity on F. Then, the map sending σ to $\varphi \circ \sigma \circ \varphi^{-1}$ defines a group isomorphism

$$\text{Gal}\left(L_1/F\right) \cong \text{Gal}\left(L_2/F\right).$$

Isomorphisms of fields were first defined by Dedekind in 1877 under the name 'permutations'. Here is his definition.

Definition 5.2 (field isomorphism). Let Ω be a field. By a permutation of Ω, we mean a substitution which changes each number

$$\alpha, \beta, \alpha+\beta, \alpha-\beta, \alpha\beta, \alpha/\beta \quad \text{of } \Omega$$

into a corresponding number

$$\alpha', \beta', (\alpha+\beta)', (\alpha-\beta)', (\alpha\beta)', (\alpha/\beta)'$$

in such a way that

$$(\alpha+\beta)' = \alpha'+\beta' \quad \text{and} \quad (\alpha\beta)' = \alpha'\beta' \quad \text{are satisfied}$$

and the substitute numbers $\alpha', \beta', \ldots$ are not all zero. The set Ω' of the latter numbers forms a new field.

We will see in Example 5.8 that

$$\sigma : \Omega \to \Omega' \quad \text{given by} \quad \alpha \mapsto \alpha' \quad \text{is an isomorphism of fields.}$$

Example 5.8 (Cox p. 129 Question 4)**.** In Definition 5.2, Dedekind defined a 'permutation' $\alpha \mapsto \alpha'$ to be a map $\Omega \to \Omega'$ satisfying

$$(\alpha+\beta)' = \alpha' + \beta' \quad \text{and} \quad (\alpha\beta)' = \alpha'\beta' \quad \text{for all } \alpha, \beta \in \Omega.$$

Dedekind also assumes that $\Omega' = \{\alpha' : \alpha \in \Omega\}$ and that the α are not all zero.

(a) Show that $1 \in \Omega$ maps to $1 \in \Omega'$. Once this is proved, it follows that $\alpha \mapsto \alpha'$ is a ring homomorphism (recall from MA3201 that sending 1 to 1 is part of the definition of ring homomorphism).

(b) Show that the map $\alpha \mapsto \alpha'$ is one-to-one.

This shows that Dedekind's definition of field isomorphism is equivalent to ours.

Solution.

(a) Let $\varphi(\alpha) = \alpha'$. Then,

$$\varphi(\alpha+\beta) = \varphi(\alpha) + \varphi(\beta) \quad \text{and} \quad \varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta).$$

So,

$$\varphi(\alpha) = \varphi(\alpha \cdot 1) = \varphi(\alpha)\varphi(1).$$

Since $\alpha' \neq 0$, then $\varphi(\alpha) = \alpha'$ has an inverse in Ω'. So, $\varphi(1) = 1$, i.e. $1 \in \Omega$ is mapped to $1 \in \Omega'$.

(b) Suppose $\varphi(\alpha_1) = \varphi(\alpha_2)$. Then, $\varphi(\alpha_1 - \alpha_2) = e_{\Omega'}$, where $e_{\Omega'}$ is the additive identity of Ω'. So, $\alpha_1 - \alpha_2 = 0$, implying that $\alpha_1 = \alpha_2$. We conclude that φ is injective. □

Definition 5.3 (Galois group of polynomial)**.** Let $f \in F[x]$. The Galois group of f over F is $\mathrm{Gal}(L/F)$, where L is a splitting field of f over F.

To check that Definition 5.3 makes sense, suppose L_1 and L_2 are splitting fields of $f \in F[x]$. By Corollary 4.1, $L_1 \cong L_2$ via an isomorphism that is the identity on F, so $\mathrm{Gal}(L_1/F) \cong \mathrm{Gal}(L_2/F)$ by Proposition 5.3. Thus, the Galois group of f over F is well-defined up to isomorphism.

Example 5.9. Recall Example 5.5, where we mentioned that $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. Note that $x^2+1 \in \mathbb{R}[x]$, so the Galois group of x^2+1 over $\mathbb{R}$ is $\mathbb{Z}/2\mathbb{Z}$.

5.2. *Galois Groups of Splitting Fields*

Recall that a polynomial $f \in F[x]$ is separable if it has distinct roots in splitting field. We now see that the order of the Galois group $\mathrm{Gal}(L/F)$ is precisely the degree of the field extension.

Theorem 5.1. Suppose L is the splitting field of a separable polynomial in $F[x]$. Then, the Galois group of $F \subseteq L$ has order

$$|\mathrm{Gal}(L/F)| = [L:F].$$

In general, if the extension $F \subseteq L$ is not a splitting field of a separable polynomial in $F[x]$, we have the inequality

$$|\mathrm{Gal}(L/F)| \leq [L:F].$$

This is not surprising by a previous example that we have just seen. Recall that in Example 5.4, we showed that the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is trivial, where $L = \mathbb{Q}\left(\sqrt[3]{2}\right)$. However, this extension is not a splitting field. Since $[L:\mathbb{Q}] = 3$ and $|\mathrm{Gal}(L/\mathbb{Q})| = 1$, the inequality $|\mathrm{Gal}(L/\mathbb{Q})| \leq [L:\mathbb{Q}]$ is satisfied — in fact, the inequality is strict in this case!

Moreover, we will see in the next chapter that if $F \subseteq L$ is a finite extension, and the hypothesis in Theorem 5.1 is satisfied, then we say that the extension $F \subseteq L$ is a Galois extension, or more simply, Galois (Definition 6.2).

Example 5.10. Consider the extension $\mathbb{Q} \subseteq L = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. In Example 5.7, we mentioned that $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is uniquely determined by

$$\sigma\left(\sqrt{2}\right) = \pm\sqrt{2} \quad \text{and} \quad \sigma\left(\sqrt{3}\right) = \pm\sqrt{3}.$$

This shows that $|\mathrm{Gal}(L/\mathbb{Q})| \leq 4$. In fact, we also showed that equality holds. By the tower theorem (Theorem 3.9), one can easily deduce that $[L:\mathbb{Q}] = 4$ and L is the splitting field of the separable polynomial $\left(x^2-2\right)\left(x^2-3\right)$. Hence, all of the above sign combinations must occur. We also showed that there exists $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ such that

$$\begin{aligned} \sigma\left(\sqrt{2}\right) &= \sqrt{2} \quad \text{and} \quad \sigma\left(\sqrt{3}\right) = -\sqrt{3} \quad \text{and} \\ \tau\left(\sqrt{2}\right) &= -\sqrt{2} \quad \text{and} \quad \tau\left(\sqrt{3}\right) = \sqrt{3} \end{aligned}$$

So, $\mathrm{Gal}(L/\mathbb{Q}) = \{1_L, \sigma, \tau, \sigma\tau\}$. In fact, one can easily deduce (to be discussed in Example 5.11) that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, for which the direct product on the right is known as the Klein four-group V (recall from MA2202).

Example 5.11 (Galois group isomorphic to V; Cox p. 131 Question 1)**.** Complete Example 5.10 by showing that

$$\mathrm{Gal}(L/\mathbb{Q}) = \{1_L, \sigma, \tau, \sigma\tau\} \quad \text{and} \quad \mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Solution. The first part was already shown in Example 5.7. For the second part, consider the map

$$\phi : \mathrm{Gal}(L/\mathbb{Q}) \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{where} \quad 1_L \mapsto (0,0), \sigma \mapsto (0,1), \tau \mapsto (1,0), \sigma\tau \mapsto (1,1).$$

It is obvious that ϕ is an isomorphism. □

5.3. *Permutations of Roots*

Cardano's formula! *Hopefully it rings a bell.* Early on in this set of notes, we saw that permutations of the roots of a cubic arise naturally from Cardano's formula. We now explain more generally how Galois groups relate to permutations. As in the previous section, we assume that L is the splitting field of a separable polynomial $f \in F[x]$. Our goal is to interpret $\text{Gal}(L/F)$ in terms of the permutations of roots of f.

Let $n = \deg(f)$. Then, in $L[x]$, we can write the product

$$f = a_0 \prod_{i=1}^{n} (x - \alpha_i) \quad \text{where } a_0 \neq 0 \text{ and } \alpha_1, \ldots, \alpha_n \in L \text{ are distinct.}$$

In this situation, we obtain a map

$$\text{Gal}(L/F) \to S_n$$

since each permutation $\sigma \in \text{Gal}(L/F)$ maps the roots of $f(x)$ to other roots, i.e. σ permutes the roots $\alpha_1, \ldots, \alpha_n$. In fact, recall that $\sigma(\alpha_i)$ is also a root of f, so that

$$\sigma(\alpha_i) = \alpha_{\tau(i)} \quad \text{for some } 1 \leq \tau(i) \leq n.$$

Since the α_i's are distinct, then $\tau(i)$ is uniquely determined. As σ is injective, then τ is also injective, which implies $\tau \in S_n$, i.e. τ is a permutation. In fact, the map $\text{Gal}(L/F) \to S_n$ described earlier is an injective group homomorphism (or monomorphism in short).

Proposition 5.4 (monomorphism from Galois group to S_n)**.** Let $n = \deg(f)$. Then, in $L[x]$, we can write the product

$$f = a_0 \prod_{i=1}^{n} (x - \alpha_i) \quad \text{where } a_0 \neq 0 \text{ and } \alpha_1, \ldots, \alpha_n \in L \text{ are distinct.}$$

Then, the map

$$\text{Gal}(L/F) \to S_n \quad \text{is an injective group homomorphism.}$$

Recall from MA1100 the following fact: if A and B are non-empty finite sets, for map $f : A \to B$,

$$f \text{ is injective} \quad \text{if and only if} \quad |A| \leq |B|.$$

One checks that $\text{Gal}(L/F)$ and S_n satisfy the aforementioned hypotheses. So, by Proposition 5.4, it follows that for the splitting field of a separable polynomial of degree n, we can regard the Galois group as a subgroup of S_n. By Lagrange's theorem, it follows that $|\text{Gal}(L/F)| \mid n!$. Since $[L:F] = |\text{Gal}(L/F)|$ by Theorem 5.1, we obtain the following corollary:

Corollary 5.2. If L is the splitting field of a separable polynomial in $f \in F[x]$, then

$$[L:F] \mid n! \quad \text{where} \quad n = \deg(f).$$

We now provides some examples of Proposition 5.4 (monomorphism from Galois group to symmetric group).

Example 5.12. Recall that the splitting field of $f = (x^2-2)(x^2-3)$ over $\mathbb{Q}$ is $L = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ and $\operatorname{Gal}(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$, where

$$\begin{aligned} \sigma\left(\sqrt{2}\right) &= \sqrt{2} \quad \text{and} \quad \sigma\left(\sqrt{3}\right) = -\sqrt{3} \quad \text{and} \\ \tau\left(\sqrt{2}\right) &= -\sqrt{2} \quad \text{and} \quad \tau\left(\sqrt{3}\right) = \sqrt{3} \end{aligned}$$

Now, let

$$\alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}, \alpha_3 = \sqrt{3}, \alpha_4 = -\sqrt{3}.$$

This is consistent with our notation in Proposition 5.4, where we mentioned that the α_i's are the roots of the polynomial $f = (x^2-2)(x^2-3)$, where each $\alpha_i \in L$. So, $\operatorname{Gal}(L/\mathbb{Q})$ is isomorphic to a subgroup of S_4 by Proposition 5.4. The automorphism σ fixes α_1 and α_2 and interchanges α_3 and α_4, which implies $\sigma \mapsto (3\,4) \in S_4$; the automorphism τ fixes α_3 and α_4 and interchanges α_1 and α_2, which implies $\tau \mapsto (1\,2) \in S_4$.

Consequently, $\sigma\tau \mapsto (1\,2)(3\,4)$, where we used the fact that disjoint cycles commute (recall from MA2202). So,

$$\operatorname{Gal}(L/\mathbb{Q}) \cong \{e, (1\,2), (3\,4), (1\,2)(3\,4)\} \subseteq S_4.$$

Example 5.13. Consider the extension

$$\mathbb{Q} \subseteq L = \mathbb{Q}\left(\omega, \sqrt[3]{2}\right) \quad \text{where } \omega = e^{2\pi i/3}.$$

Since L is the splitting field of x^3-2 over $\mathbb{Q}$, we obtain an injective group homomorphism $\operatorname{Gal}(L/\mathbb{Q}) \hookrightarrow S_3$ (recall that the hook denotes an injective map). Recall that $[L:\mathbb{Q}] = 6$. Since $[L:\mathbb{Q}] = |\operatorname{Gal}(L/\mathbb{Q})|$ (Theorem 5.1; check that the hypothesis is satisfied), it follows that $\operatorname{Gal}(L/\mathbb{Q}) \cong S_3$ since $|S_3| = 6$.

When one thinks of Galois groups in terms of permutations, it makes sense to ask how

properties of the permutations relate to properties of the corresponding field extension.

One nice example of this involves transitive subgroups of S_n. We now give its definition.

Definition 5.4 (transitive subgroup)**.** Let $H \leq S_n$. We say that H is transitive if

$$\text{for every pair of } i, j \in \{1, \ldots, n\} \quad \text{there exists} \quad \tau \in H \text{ such that } \tau(i) = j.$$

Example 5.14. A trivial example is that S_n is a transitive subgroup of itself since the transpostiion $(i\, j)$ takes i to j. However, not all subgroups of S_n are transitive.

Example 5.15. The subgroup

$$\{e, (1\,2), (3\,4), (1\,2)(3\,4)\} \leq S_4 \quad \text{is not transitive.}$$

To see why, no element of the subgroup sends 1 to 3.

It is natural to ask if the subgroup of S_n corresponding to $\mathrm{Gal}(L/F)$ is transitive.

Proposition 5.5 (Jordan)**.** Let F be the splitting field of a separable polynomial $f \in F[x]$ of degree n. Then, the subgroup of S_n corresponding to $\mathrm{Gal}(L/F)$ is transitive if and only if f is irreducible over F.

Definition 5.4 defines a transitive subgroup of S_n. In fact, this can be generalised to any group action, i.e. if a group G acts on a set X, then the action is transitive if

$$\text{for all } x, y \in X \quad \text{there exists } g \in G \quad \text{such that} \quad g \cdot x = y.$$

For example, if L is the splitting field of a separable polynomial $f \in F[x]$, then $\mathrm{Gal}(L/F)$ acts on the roots of f. As such, Jordan's proposition (Proposition 5.5) can be restated as follows:

$$f \text{ is irreducible} \quad \text{if and only if} \quad \mathrm{Gal}(L/F) \text{ acts transitively on the roots of } F.$$

6. The Galois Correspondence

6.1. *Galois Extensions*

Previously, we learnt that splitting fields of separable polynomials are especially nice from the perspective of Galois theory. We now wish to characterise such extensions in terms of normality and separability. We will also apply this theory to study separable extensions.

Before delving into the main results, we introduce the idea of a fixed field.

Definition 6.1 (fixed field). Suppose we have a finite extension $F \subseteq L$ with Galois group $\text{Gal}(L/F)$. Given a subgroup $H \leq \text{Gal}(L/F)$, we call

$$L_H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\} \quad \text{to be the fixed field of } H.$$

Theorem 6.1. Let $F \subseteq L$ be a finite extension. Then, the following are equivalent:

(a) L is the splitting field of a separable polynomial in $F[x]$

(b) F is the fixed field of $\text{Gal}(L/F)$ acting on L

(c) $F \subseteq L$ is a normal separable extension

Definition 6.2 (Galois extension). An extension $F \subseteq L$ is Galois if

$$\text{it is finite} \quad \text{and it satisfies any of the conditions in Theorem 6.1.}$$

We give an example of a Galois (Example 6.1) and a non-Galois extension (Example 6.2).

Example 6.1 (a Galois extension). The extension

$$\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \quad \text{is Galois.}$$

To see why, $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ is the splitting field of $\left(x^2-2\right)\left(x^2-3\right)$ over $\mathbb{Q}$. By **(a)** of Theorem 6.1, since the polynomial is separable, it follows that the extension is Galois.

Example 6.2 (a non-Galois extension). The extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt[3]{2}\right)$ is not Galois since x^3-2 is irreducible over $\mathbb{Q}$. Also, although x^3-2 has a root in $\mathbb{Q}\left(\sqrt[3]{2}\right)$, it does not split completely over $\mathbb{Q}\left(\sqrt[3]{2}\right)$. Recall Definition 4.2 on what it means for an extension to be normal — one of the hypotheses requires the polynomial in the extension field to split completely, but as mentioned, this is not satisfied, making the extension not normal. By **(c)** of Theorem 6.1, the result follows.

Proposition 6.1. Suppose $F \subseteq L$ is a Galois extension and that we have an intermediate field K satisfying $F \subseteq K \subseteq L$. Then, $K \subseteq L$ is also a Galois extension.

It is interesting to note that in Proposition 6.1, although

$$F \subseteq L \text{ and } K \subseteq L \text{ are Galois} \quad \text{it does not imply that} \quad F \subseteq K \text{ is Galois.}$$

We will see an example of this in Example 6.3.

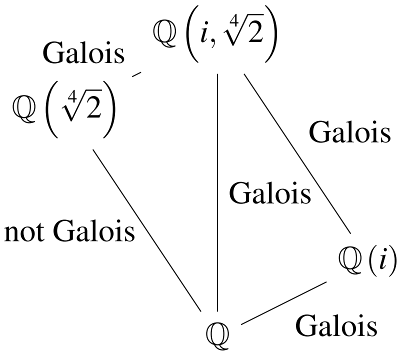
Example 6.3. Recall that

$$\mathbb{Q} \subseteq \mathbb{Q}\left(i, \sqrt[4]{2}\right) \quad \text{is the splitting field of } x^4 - 2.$$

So, the extension is Galois. Consider the intermediate fields $\mathbb{Q}(i)$ and $\mathbb{Q}\left(\sqrt[4]{2}\right)$. Then, $\mathbb{Q} \subseteq \mathbb{Q}(i)$ is Galois as it is the splitting field of x^2+1, but $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt[4]{2}\right)$ is not because x^4-2 is the minimal polynomial of $\sqrt[4]{2}$ which does not split completely. Also, one checks that

$$\mathbb{Q}\left(\sqrt[4]{2}\right) \subseteq \mathbb{Q}\left(i, \sqrt[4]{2}\right) \text{ and } \mathbb{Q}(i) \subseteq \mathbb{Q}\left(i, \sqrt[4]{2}\right) \quad \text{are Galois.}$$

To summarise, we have the following diagram:


$\mathbb{Q}\left(i, \sqrt[4]{2}\right)$
Galois
$\mathbb{Q}\left(\sqrt[4]{2}\right)$
Galois
Galois
not Galois
$\mathbb{Q}(i)$
$\mathbb{Q}$
Galois

We know that

$$F \subseteq L \text{ is Galois} \quad \text{implies} \quad |\mathrm{Gal}(L/F)| = [L : F].$$

For arbitrary finite extensions, the relation between the order of the Galois group and the degree of the extension can be described as follows:

Theorem 6.2. Let $F \subseteq L$ be a finite extension. Then, the following hold:

(a) $|\mathrm{Gal}(L/F)| \mid [L : F]$

(b) $|\mathrm{Gal}(L/F)| \leq [L : F]$

(c) $F \subseteq L$ is a Galois extension if and only if $|\mathrm{Gal}(L/F)| = [L : F]$

Proposition 6.2. Let $F \subseteq L$ be a finite extension. Then, L is separable over F if and only if $L = F(\alpha_1, \ldots, \alpha_n)$, where each α_i is separable over F.

We then introduce the idea of a Galois closure.

Proposition 6.3. Let $F \subseteq L$ be a finite separable extension. Then, there is an extension $L \subseteq M$ such that the following hold:

(a) M is Galois over F, i.e. $F \subseteq M$ is a Galois extension

(b) Given any other extension $L \subseteq M'$ such that M' is Galois over F, there is a field homomorphism $\varphi : M \to M'$ that is the identity on L.

6.2. *Normal Subgroups and Normal Extensions Revisited*

Previously, we introduced the idea of a normal extension. Also, in MA2202, normal subgroups were discussed. In fact, it is not a coincidence that these concepts have the same name. We begin our discussion with conjugate fields.

Recall from O-Level that

$$2-\sqrt{3} \quad \text{is the conjugate of} \quad 2+\sqrt{3}.$$

We have an analogous definition for subfields.

Definition 6.3 (conjugate field)**.** Let $F \subseteq K \subseteq L$ be finite extensions. Suppose $\sigma \in \mathrm{Gal}\left(L/F\right)$ is an automorphism. Then,

$$\sigma K = \left\{\sigma\left(\alpha\right) : \alpha \in K\right\} \quad \text{is a conjugate field of } K.$$

Technically, we should write $\sigma\left(K\right)$ instead of σK but we would prefer the latter because it is less cumbersome. Since σ is a field isomorphism, it follows that σK is subfield of L.

Lemma 6.1. Let $F \subseteq K \subseteq L$ and $\sigma \in \mathrm{Gal}\left(L/F\right)$. Then,

$$F \subseteq \sigma K \subseteq L \quad \text{and} \quad \left[L:F\right] = \left[\sigma K : F\right].$$

We now provide an example of conjugate fields.

Example 6.4 (conjugate field)**.** Consider the extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\omega, \sqrt[3]{2}\right)$, where $\omega = e^{2\pi i/3}$. Then, we have the following intermediate fields:

$$\begin{tikzcd}
 & \mathbb{Q}\left(\omega, \sqrt[3]{2}\right) & & \\
\mathbb{Q}\left(\omega\right) \arrow[ur] & \mathbb{Q}\left(\sqrt[3]{2}\right) \arrow[u] & \mathbb{Q}\left(\omega\sqrt[3]{2}\right) \arrow[ul] & \mathbb{Q}\left(\omega^2\sqrt[3]{2}\right) \arrow[ull] \\
 & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

Well, let $L = \mathbb{Q}\left(\omega, \sqrt[3]{2}\right)$. Then, $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is uniquely determined by

$$\sigma(\omega) \in \left\{\omega, \omega^2\right\} \quad \text{and} \quad \sigma\left(\sqrt[3]{2}\right) \in \left\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\right\}.$$

In fact (This is from Exercise 2 of Section 6.2 of Cox's book, remember to add here), all possible combinations of $\sigma(\omega)$ and $\sigma\left(\sqrt[3]{2}\right)$ actually occur. In fact, we will see in Example 6.5 that the following hold:

- **(a)** $\mathbb{Q}\left(\sqrt[3]{2}\right)$ has conjugate fields $\mathbb{Q}\left(\sqrt[3]{2}\right)$, $\mathbb{Q}\left(\omega\sqrt[3]{2}\right)$, and $\mathbb{Q}\left(\omega^2\sqrt[3]{2}\right)$
- **(b)** $\mathbb{Q}(\omega)$ equals all of its conjugates

Example 6.5 (Cox p. 160 Question 1)**.** In the diagram shown in Example 6.4, verify the following:

- **(a)** $\mathbb{Q}\left(\sqrt[3]{2}\right)$ has conjugate fields $\mathbb{Q}\left(\sqrt[3]{2}\right)$, $\mathbb{Q}\left(\omega\sqrt[3]{2}\right)$, and $\mathbb{Q}\left(\omega^2\sqrt[3]{2}\right)$
- **(b)** $\mathbb{Q}(\omega)$ equals all of its conjugates

Solution.

(a) Note that there exist $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ such that

$$\sigma(\omega) = \omega \text{ and } \sigma\left(\sqrt[3]{2}\right) = \omega\sqrt[3]{2} \quad \text{and} \quad \tau(\omega) = \omega^2 \text{ and } \tau\left(\sqrt[3]{2}\right) = \omega^2\sqrt[3]{2}.$$

Let $G = \mathrm{Gal}(L/\mathbb{Q}) = \langle\sigma, \tau\rangle$. Define $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$. We show that $\sigma K = \mathbb{Q}\left(\omega\sqrt[3]{2}\right)$. If $\beta \in \sigma K$, then we can write $\beta = \sigma(\alpha)$, where $\alpha \in K$, so $\alpha = p\left(\sqrt[3]{2}\right)$, where $p \in \mathbb{Q}[x]$. Also, $\beta = \sigma\left(p\left(\sqrt[3]{2}\right)\right) = p\left(\omega\sqrt[3]{2}\right)$, which implies $\sigma K \subseteq \mathbb{Q}\left(\omega\sqrt[3]{2}\right)$. The proof of the reverse inclusion is similar.

Now that we have deduced that

$$\sigma K = \mathbb{Q}\left(\omega\sqrt[3]{2}\right) \quad \text{it follows that} \quad \sigma^2 K = \mathbb{Q}\left(\omega^2\sqrt[3]{2}\right).$$

Consequently, $eK = K$. As such, we have shown that the three mentioned fields are indeed conjugate fields of $\mathbb{Q}\left(\sqrt[3]{2}\right)$. Moreover, as $\tau K = K$ and $G = \langle\sigma, \tau\rangle$, it follows that the conjugate fields are unique.

(b) Since $\sigma(\omega) = \omega$ and σ is the identity on $\mathbb{Q}$, then $\sigma\mathbb{Q}(\omega) = \mathbb{Q}(\omega)$. Moreover, $\tau\mathbb{Q}(\omega) = \mathbb{Q}\left(\omega^2\right)$. As $\omega^2 + \omega + 1 = 0$, it follows that $\omega^2 = -1 - \omega$, so $\mathbb{Q}\left(\omega^2\right) = \mathbb{Q}(\omega)$. As

$$\sigma\mathbb{Q}(\omega) = \mathbb{Q}(\omega) \quad \text{and} \quad \tau\mathbb{Q}(\omega) = \mathbb{Q}(\omega) \quad \text{and } G = \langle\sigma, \tau\rangle,$$

it follows that $\lambda\mathbb{Q}(\omega) = \mathbb{Q}(\omega)$ for all $\lambda \in \mathrm{Gal}(L/F)$. □

We then relate intermediate fields to subgroups of the Galois group. We see in **(b)** of Lemma 6.2 that conjugate fields correspond to conjugate subgroups. This is analogous to the concept of the conjugate of a subgroup $H \leq G$ in MA2202, which is defined to be a subgroup of the form gHg^{-1} for some $g \in G$.

Lemma 6.2. Suppose we have finite extensions $F \subseteq K \subseteq L$. Then, the following hold:

(a) $\operatorname{Gal}(L/K) \leq \operatorname{Gal}(L/F)$

(b) If $\sigma \in \operatorname{Gal}(L/F)$, then $\operatorname{Gal}(L/\sigma K) = \sigma \operatorname{Gal}(L/K)\sigma^{-1}$ in $\operatorname{Gal}(L/F)$

We will see in Theorem 6.3 that we have certain equivalent statements. In particular, normal subgroups are somehow related to normal extensions.

Theorem 6.3. Suppose we have fields $F \subseteq K \subseteq L$, where $F \subseteq L$ is a Galois extension. Then, the following conditions are equivalent:

(a) $K = \sigma K$ for all $\sigma \in \operatorname{Gal}(L/F)$, i.e. K equals all of its conjugates

(b) $\operatorname{Gal}(L/K) \trianglelefteq \operatorname{Gal}(L/F)$

(c) $F \subseteq K$ is a Galois extension

(d) $F \subseteq K$ is a normal extension

Let us see an application of Theorem 6.3.

Example 6.6. Consider $\mathbb{Q} \subseteq L = \mathbb{Q}\left(\omega, \sqrt[3]{2}\right)$. Then, there exist automorphisms $\sigma, \tau \in \operatorname{Gal}(L/\mathbb{Q})$ such that

$$\sigma(\omega) = \omega \text{ and } \sigma\left(\sqrt[3]{2}\right) = \omega\sqrt[3]{2} \quad \text{and} \quad \tau(\omega) = \omega^2 \text{ and } \tau\left(\sqrt[3]{2}\right) = \sqrt[3]{2}.$$

Label the roots of $x^3 - 2$ as

$$\alpha_1 = \sqrt[3]{2} \quad \alpha_2 = \omega\sqrt[3]{2} \quad \alpha_3 = \omega^2\sqrt[3]{2}.$$

Consider the isomorphism $\operatorname{Gal}(L/\mathbb{Q}) \cong S_3$ given by the action of the automorphisms on the roots $\alpha_1, \alpha_2, \alpha_3$. Then, we see that $\sigma \mapsto (1\,2\,3)$ and $\tau \mapsto (2\,3)$. Since these permutations generate S_3, it follows that σ and τ generate $\operatorname{Gal}(L/\mathbb{Q})$.

Recall the following diagram. Each such field K gives a subgroup $\operatorname{Gal}(L/K) \subseteq \operatorname{Gal}(L/\mathbb{Q})$. Moreover,

$$K_1 \subseteq K_2 \subseteq L \quad \text{implies} \quad \operatorname{Gal}(L/K_1)\operatorname{Gal}(L/K_2).$$

$$\begin{tikzcd}
& \mathbb{Q}\left(\omega, \sqrt[3]{2}\right) & & \\
\mathbb{Q}(\omega) \arrow[ur] & \mathbb{Q}\left(\sqrt[3]{2}\right) \arrow[u] & \mathbb{Q}\left(\omega\sqrt[3]{2}\right) \arrow[ul] & \mathbb{Q}\left(\omega^2\sqrt[3]{2}\right) \arrow[ull] \\
& \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

In other words, larger fields correspond to smaller Galois groups. Then, we claim that for the fields K in the in the diagram above, the map $K \mapsto \operatorname{Gal}(L/K)$ yields the following diagram of subgroups of

$\mathrm{Gal}(L/\mathbb{Q})$. This is precisely the Galois correspondence!

$$\begin{tikzcd}
 & & \{e\} \arrow[dll] \arrow[dl] \arrow[dr] \arrow[drr] & & \\
\langle\sigma\rangle \arrow[drr] & \langle\tau\rangle \arrow[dr] & & \langle\sigma^2\tau\rangle \arrow[dl] & \langle\sigma\tau\rangle \arrow[dll] \\
 & & \mathrm{Gal}(L/\mathbb{Q}) & &
\end{tikzcd}$$

In this diagram, $\langle\sigma\rangle$ is the subgroup generated by σ. Thus, $\langle\sigma\rangle = \left\{e,\sigma,\sigma^2\right\}$ since σ has order 3. Similarly, $\langle\tau\rangle, \left\langle\sigma^2\tau\right\rangle, \langle\sigma\tau\rangle$ are subgroups of order 2.

To see how these two diagrams are related, consider the case of $\mathbb{Q}(\omega)$. We know that

$$|\mathrm{Gal}(L/\mathbb{Q}(\omega))| = [L:\mathbb{Q}(\omega)] = \left[\mathbb{Q}\left(\omega,\sqrt[3]{2}\right):\mathbb{Q}(\omega)\right] = \frac{\left[\mathbb{Q}\left(\omega,\sqrt[3]{2}\right):\mathbb{Q}\right]}{[\mathbb{Q}(\omega):\mathbb{Q}]} = \frac{6}{2} = 3.$$

Moreover, σ is the identity on $\mathbb{Q}(\omega)$ since $\sigma(\omega) = \omega$. Thus, $\sigma \in \mathrm{Gal}(L/\mathbb{Q}(\omega))$, and it follows easily that $\mathrm{Gal}(L/\mathbb{Q}(\omega)) = \langle\sigma\rangle$.

In Group Theory, normal subgroups are important as they lead to quotient groups. Recall that if $N \trianglelefteq G$, then left cosets of N coincide with right cosets, and the set G/N consisting of all cosets of N in G becomes a group under multiplication, the quotient group.

When $\mathrm{Gal}(L/K) \subseteq \mathrm{Gal}(L/F)$ is normal, the second main theorem of this section explains how to interpret the quotient group.

Theorem 6.4. Suppose we have extension fields $F \subseteq K \subseteq L$, where $F \subseteq K$ and $F \subseteq L$ are Galois. Then, $\mathrm{Gal}(L/K) \trianglelefteq \mathrm{Gal}(L/F)$, and there exists a natural isomorphism of groups

$$\mathrm{Gal}(L/F)\,\mathrm{Gal}(L/K) \cong \mathrm{Gal}(K/F).$$

Example 6.7. Consider

$$\mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq L = \mathbb{Q}\left(\omega,\sqrt[3]{2}\right).$$

Since $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ is Galois and $\mathrm{Gal}(L/\mathbb{Q}(\omega)) = \langle\sigma\rangle$, where $\sigma(\omega) = \omega$ and $\sigma\left(\sqrt[3]{2}\right) = \omega\sqrt[3]{2}$. Then by Theorem 6.4,

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q})/\langle\sigma\rangle.$$

Note that $\sigma \mapsto (1\,2\,3)$, so it follows that

$$\mathrm{Gal}(L/\mathbb{Q})/\langle\sigma\rangle \cong S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}.$$

6.3. *The Fundamental Theorem of Galois Theory*

We can now state the main result of this chapter, which describes precisely the relation between subgroups and subfields. Recall that if we are given a finite extension $F \subseteq L$ and a subgroup $H \leq \mathrm{Gal}(L/F)$, then we have the fixed field

$$L_H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

We now state the Fundamental Theorem of Galois Theory.

Theorem 6.5 (Fundamental Theorem of Galois Theory). Let $F \subseteq L$ be a Galois extension. Then, the following hold:

(i) For an intermediate field $F \subseteq K \subseteq L$, its Galois group $\mathrm{Gal}(L/K) \subseteq \mathrm{Gal}(L/F)$ has fixed field $L_{\mathrm{Gal}(L/K)} = K$. Furthermore,

$$|\mathrm{Gal}(L/K)| = [L:K] \quad \text{and} \quad |\mathrm{Gal}(L/F) : \mathrm{Gal}(L/K)] = [K:F].$$

(ii) For a subgroup $H \leq \mathrm{Gal}(L/F)$, its fixed field $F \subseteq L_H \subseteq L$ has Galois group $\mathrm{Gal}(L/L_H) = H$. Furthermore,

$$[L:L_H] = |H| \quad \text{and} \quad [L_H:F] = [\mathrm{Gal}(L/F):H].$$

(iii) The maps between

$$\text{intermediate fields } F \subseteq K \subseteq L \quad \text{and} \quad \text{subgroups } H \subseteq \mathrm{Gal}(L/F)$$

given by the reverse inclusions

$$K \mapsto \mathrm{Gal}(L/K) \quad \text{and} \quad H \mapsto L_H \quad \text{are inverses of each other.}$$

Furthermore, if a subfield K corresponds to a subgroup H under these maps, then K is Galois over F if and only if $H \trianglelefteq \mathrm{Gal}(L/F)$, and when this happens, there exists a natural isomorphism

$$\mathrm{Gal}(L/F)/H \cong \mathrm{Gal}(K/F).$$

We now give two examples of the Galois correspondence.

Example 6.8. Consider the extension

$$\mathbb{Q} \subseteq L = \mathbb{Q}\left(\omega, \sqrt[3]{2}\right) = e^{2\pi i/3}.$$

Recall that $\mathrm{Gal}\,(L/\mathbb{Q}) \cong S_3$ has subgroups as follows:

$$\begin{tikzcd}
 & \{e\} \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] & & \\
\langle\sigma\rangle \arrow[dr] & \langle\tau\rangle \arrow[d] & \langle\sigma^2\tau\rangle \arrow[dl] & \langle\sigma\tau\rangle \arrow[dll] \\
 & \mathrm{Gal}\,(L/\mathbb{Q}) & &
\end{tikzcd}$$

where

$$\sigma\,(\omega) = \omega \text{ and } \sigma\left(\sqrt[3]{2}\right) = \omega\sqrt[3]{2} \quad \text{and} \quad \tau\,(\omega) = \omega^2 \text{ and } \tau\left(\sqrt[3]{2}\right) = \sqrt[3]{2}.$$

In fact, these are all the subgroups of $\mathrm{Gal}\,(L/\mathbb{Q})$. The corresponding fixed fields are as follows:

$$\begin{tikzcd}
 & \mathbb{Q}\left(\omega,\sqrt[3]{2}\right) & & \\
\mathbb{Q}\,(\omega) \arrow[ur] & \mathbb{Q}\left(\sqrt[3]{2}\right) \arrow[u] & \mathbb{Q}\left(\omega\sqrt[3]{2}\right) \arrow[ul] & \mathbb{Q}\left(\omega^2\sqrt[3]{2}\right) \arrow[ull] \\
 & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

The key point is that by **(iii)** of the Fundamental Theorem of Galois Theory (Theorem 6.5), these are all the subfields of $L = \mathbb{Q}\left(\omega,\sqrt[3]{2}\right)$ containing $\mathbb{Q}$.

Here is a more complicated example (to be included, which comes from Example 7.3.4 of Cox's textbook and we will link to the relevant exercise).

Example 6.9. Let $f\,(x) \in \mathbb{Q}\,[x]$ be an irreducible polynomial and L be the splitting field of $f\,(x)$ over $\mathbb{Q}$. Show that

$$\text{if } \mathrm{Gal}\,(L/\mathbb{Q}) \cong C_3 \quad \text{then} \quad \text{all the roots of } f\,(x) \text{ are real.}$$

Solution. We have either $\mathrm{Gal}\,(L \mid \mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$ or $\mathrm{Gal}\,(L \mid \mathbb{Q}) = S_3$, depending on whether there is an automorphism swapping two roots. In our case, there is no automorphism swapping two roots since a cyclic group of order 3 has no subgroup of order 2. If f has a root $z \in \mathbb{C}$, then $\bar{z}$ would also be a root and $z \mapsto \bar{z}$ would be an automorphism. As such, no automorphism $z \mapsto \bar{z}$ can exist, implying all roots of f must be real. □

Example 6.10. Let $g(x)$ be an irreducible quartic polynomial in $\mathbb{Q}[x]$ with Galois Group G. Show that if $g(x)$ has two real roots, then $G \cong S_4$ or $G \cong D_8$.

Solution. Since $\deg(g) = 4$, then G admits one of the following possibilities: Z_4, V_4, D_8, A_4, S_4. As g has two real roots, then it has two complex roots that occur in conjugate pairs because $g \in \mathbb{Q}[x]$. Since complex conjugate roots are equivalent to the conjugation of a transposition, and the only transitive subgroups containing a transposition are D_8 and S_4, we are done. □

We then give an interesting application of the Galois correspondence.

Proposition 6.4. Let $F \subseteq L$ be a finite separable extension. Then, there exist only finitely many intermediate fields K such that $F \subseteq K \subseteq L$.

In contrast, there are finite purely inseparable extensions that have infinitely many intermediate fields. We provide a classic example.

Example 6.11. Let k be a field of characteristic p, and consider the extension

$$F = k(t,u) \subseteq L.$$

Here, L is the splitting field of $(x^p - t)(x^p - u) \in F[x]$. Recall that this extension has no primitve element. Moroever, $F \subseteq L$ is purely inseparable and $L = F(\alpha, \beta)$, where $\alpha^p = t$ and $\beta^p = u$.

Also, the intermediate fields

$$F \subseteq F(\alpha + \lambda\beta) \subseteq L \quad \text{are all distinct as } \lambda \text{ ranges over the distinct elements of } F.$$

Note that F is infinite. So, there exist many intermediate fields. $\operatorname{Gal}(L/F)$ is trivial, which implies it has only one subgroup $\{e\}$, yet $F \subseteq L$ has infinitely many intermediate fields.

The Galois correspondence has a nice application to the discriminant. Recall that we defined the discriminant $\Delta(f) \in F$ of a non-constant monic polynomial $f \in F[x]$. We showed that if $\deg(f) = n$, where $n \geq 2$, and

$$f = \prod_{i=1}^{n} (x - \alpha_i) \text{ in a splitting field } L \text{ of } f \quad \text{then} \quad \Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in F.$$

Recall that by Proposition 4.3,

$$f \text{ is separable} \quad \text{if and only if} \quad \Delta(f) \neq 0.$$

We define

$$\sqrt{\Delta(f)} = \prod_{i<j} (\alpha_i - \alpha_j) \in L.$$

Note that while $\Delta(f)$ is uniquely determined by f, the above square root depends on how the roots are labelled. Also, recall when we introduced Galois groups, if $f \in F[x]$ is separable, then the action of the Galois group on the roots $\alpha_1, \ldots, \alpha_n$ of f gives an injective group homomorphism

$$\operatorname{Gal}(L/F) \hookrightarrow S_n.$$

In S_n, we also have the alternating group $A_n \leq S_n$. We give the following result that $\sqrt{\Delta(f)}$ *controls* the relation between A_n and $\operatorname{Gal}(L/F)$.

Theorem 6.6. Let $f \in F[x]$ be of degree $n \geq 2$ and $f = (x - \alpha_1) \ldots (x - \alpha_n)$ in a splitting field L of f. Assume $\operatorname{char}(F) \neq 2$. Then, the following hold:

(a) If $\sigma \in \operatorname{Gal}(L/F)$ corresponds to $\tau \in S_n$, then

$$\sigma\left(\sqrt{\Delta(f)}\right) = \operatorname{sgn}(\tau)\sqrt{\Delta(f)}$$

(b) The image of $\operatorname{Gal}(L/F)$ lies in A_n if and only if $\sqrt{\Delta(f)} \in F$

As such, we are able to compute the Galois group of an irreducible cubic.

Proposition 6.5 (Galois group of irreducible separable cubic)**.** Let $f \in F[x]$ be a monic irreducible separable cubic, where $\operatorname{char}(F) \neq 2$. If L is the splitting field of f over F, then

$$\operatorname{Gal}(L/F) \cong \begin{cases} \mathbb{Z}/3\mathbb{Z} & \text{if } \Delta(f) \text{ is a square in } F; \\ S_3 & \text{otherwise.} \end{cases}$$

Example 6.12. Consider

$$f = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x] \quad \text{which is irreducible over } \mathbb{Q}.$$

As such, f is separable since $\operatorname{char}(\mathbb{Q}) = 0 \neq 2$. Since $\operatorname{Delta}(f) = 49 = 7^2$, it follows that the Galois group of f over $\mathbb{Q}$ is cyclic of order 3, i.e. the group is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

We have a more general case of Proposition 6.5, which is when the cubic is just irreducible over F.

Proposition 6.6 (Galois group of irreducible cubic)**.** The Galois group of an irreducible cubic $\in \mathbb{Q}[x]$ is isomorphic to S_3 or $\mathbb{Z}_3$.

Proof. Let G denote the Galois group. Since the cubic polynomial is irreducible over $\mathbb{Q}$, we consider a field extension of degree n, where $2 \leq n \leq 6$. By the tower theorem, $n \mid 6$ so $n = 2, 3$ or 6. We consider two cases.

- **Case 1:** If $n = 3$, then $G \cong \mathbb{Z}_3$
- **Case 2:** If $n = 6$, then $G \cong S_3$ or $\mathbb{Z}_6$. For G to be isomorphic to $\mathbb{Z}_6$, G would need to have an element of order 6 but it cannot have elements of order greater than 3. Therefore, G can only be isomorphic to S_3

Lastly, we show that $n \neq 2$. If $n = 2$, then the degree of the field extension is 2, so one of the roots is the root of a quadratic, but then the cubic would not be irreducible! □

7. Solvability by Radicals

7.1. *Solvable Groups*

In this chapter, we will used the Galois theory that was previously developed to determine when a polynomial equation can be solved by radicals. The idea is to translate the problem into Group Theory. As such, we begin with the group-theoretic concept of a solvable group (Definition 7.1), which might have been covered in MA2202.

Definition 7.1 (solvable group). A finite group G is solvable if there exist subgroups

$$\{e\} = G_n \subseteq G_{n-1} \subseteq \ldots \subseteq G_1 \subseteq G_0 = G$$

where for all $1 \leq i \leq n$, we have

$$G_i \trianglelefteq G_{i-1} \quad \text{and} \quad [G_{i-1} : G_i] \text{ is prime.}$$

In the second part of Definition 7.1, since $G_i \trianglelefteq G_{i-1}$, recall from MA2202 that this is equivalent to saying that G_{i-1}/G_i is a cyclic group of prime order. Eventually, we will provide a result (Proposition 7.2) that every finite Abelian group is solvable. We now give an example of a non-Abelian solvable group.

Example 7.1. Consider the inclusions

$$\{e\} \subseteq A_3 \subseteq S_3.$$

We have $\{e\} \trianglelefteq A_3$ trivially and $A_3 \trianglelefteq S_3$ by definition of the alternating group. Moreover, as $|A_3| = 3$ and $|S_3| = 6$, it follows that

$$[A_3 : \{e\}] = 3 \text{ and } [S_3 : A_3] = 2 \text{ are prime.}$$

In fact, we will see that A_4 and S_4 is solvable but A_n and S_n are non-solvable for $n \geq 5$. Here is our first result on solvability.

Proposition 7.1. Every subgroup of a solvable finite group is solvable.

Here is one of the main theoretical tools for dealing with solvable groups.

Theorem 7.1. Let G be a finite group and $H \trianglelefteq G$. Then,

$$G \text{ is solvable} \quad \text{if and only if} \quad H \text{ and } G/H \text{ are.}$$

Proposition 7.2. Every finite Abelian group G is solvable.

Proof. Recall that the subgroup of any Abelian Group G is normal. Thus, $\{e\} \trianglelefteq G$. Now, we need to show that $G/\{e\} \cong G$, which follows from the first isomorphism theorem for groups. In fact, $G/\{e\} = G$. □

The definition of solvability is related to the ideas of simple groups, composition series, and the Jordan–Hölder theorem. We will say more about these topics in due course (still the same chapter). However, some standard results used to study solvable groups need to be mentioned here.

In some cases, the solvability of a group is determined by its order. For example, there is a result which states that

if p is prime then every group of order p^n is solvable, where $n \geq 0$.

In fact, Burnside generalised the above-mentioned result in 1904.

Theorem 7.2 (Burnside's theorem)**.** If p and q are distinct primes, then every group of order $p^n q^m$ is solvable, where $n, m \geq 0$.

In 1963, Feit and Thompson proved the following surprising result (Theorem 7.3). Although it is a simple statement, the proof uses some sophisticated Mathematics and comprises 255 pages.

Theorem 7.3 (Feit-Thompson theorem)**.** Every group of odd order is solvable.

The Sylow theorems also imply some nice results about solvability. These were mainly discussed in MA2202 so we will not state them here (remember to add Examples 8.1.10 and 8.1.11 from Cox's book to the MA2202 notes).

7.2. *Radical and Solvable Extensions*

We then introduce the Field Theory needed to study solvability by radicals. The naive idea of solvability by radicals arises from polynomials such as $x^3 + 3x + 1$, whose unique root is

$$\sqrt[3]{\frac{1}{2}\left(-1+\sqrt{5}\right)} + \sqrt[3]{\frac{1}{2}\left(-1-\sqrt{5}\right)} \quad \text{by Cardano's formula.}$$

This algebraic number is built by taking successive radicals. When we cast this in terms of fields, we are led to the following definition on what it means for a field extension to be radical.

Definition 7.2 (radical extension)**.** A field extension $F \subseteq L$ is radical if there exist fields

$$F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_{n-1} \subseteq F_n = L,$$

where for $1 \leq i \leq n$, there is $\gamma_i \in F$ with $F_i = F_{i-1}(\gamma_i)$ and $\gamma_i^{m_i} \in F_{i-1}$ and $m_i > 0$.

Observe that if we let $b_i = \gamma_i^{m_i} \in F_{i-1}$, then γ_i is an m^{th} root of b_i, i.e. $\gamma_i = \sqrt[m_i]{b_i}$, so that

$$F_i = F_{i-1}\left(\sqrt[m_i]{b_i}\right) \quad \text{where } b_i \in F_{i-1}.$$

This shows that radical extensions are obtained by adjoining successive radicals. We now provide our first example of a radical extension.

Example 7.2. Consider the field extension

$$\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right).$$

Let $\gamma_1 = \sqrt{2}$ and $\gamma_2 = \sqrt{2+\sqrt{2}}$. Then, we obtain the extension

$$\mathbb{Q} \subseteq \mathbb{Q}(\gamma_1) = \mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}\left(\sqrt{2}\right)(\gamma_2) = \mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt{2+\sqrt{2}}\right).$$

Here,

$$\gamma_1^2 = \sqrt{2}^2 = 2 \in \mathbb{Q} \quad \text{and} \quad \gamma_2^2 = \left(\sqrt{2+\sqrt{2}}\right)^2 = 2+\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right).$$

One can easily verify that $\mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt{2+\sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$, which implies that the extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ is a radical extension.

An important observation is that some extensions are not radical but contained in larger radical extensions. Here is an example.

Example 7.3. Let $\mathbb{Q} \subseteq L$ be a splitting field of $f = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$. In Example 6.12, we mentioned that f is irreducible over $\mathbb{Q}$ with discriminant $\Delta(f) = 49 = 7^2 > 0$. As such, the roots of f are real, which allows us to assume that $L \subseteq \mathbb{R}$.

Furthermore, since $\Delta(f)$ is a perfect square, then $\mathbb{Q} \subseteq L$ is a Galois extension of degree 3, i.e. the Galois group $\text{Gal}(L/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. By Cardano's formula, $\mathbb{Q} \subseteq L$ is contained in a radical extension.

However, the extension $\mathbb{Q} \subseteq L$ is not radical. Suppose on the contrary that $\mathbb{Q} \subseteq L$ is radical. Then, $[L : \mathbb{Q}] = 3$ would imply that $L = \mathbb{Q}(\gamma)$, where $\gamma^m \in \mathbb{Q}$ for some $m \geq 3$. As such, the minimal polynomial f of γ over $\mathbb{Q}$ would divide $x^m - \gamma^m$ and have degree $[L : \mathbb{Q}] = 3$. Since $\mathbb{Q} \subseteq L$ is Galois, then f would split completely over $\mathbb{Q}(\gamma)$ so that three of $\gamma, \zeta_m\gamma, \zeta_m^2\gamma, \ldots, \zeta_m^{m-1}\gamma$ would lie in L. However, this is impossible as $L \subseteq \mathbb{R}$, reaching a contradiction.

This example motivates the following definition.

Definition 7.3 (solvable extension)**.** A field extension $F \subseteq L$ ois solvable (or solvable by radicals) if there exists a field extension $L \subseteq M$ such that $F \subseteq M$ is radical.

Example 7.4. The extension $\mathbb{Q} \subseteq L$ considered in Example 7.3 is solvable since it is contained in a radical extension.

Next, to understand radical and solvable extensions, we need to define the compositum of two or more subfields.

Definition 7.4 (compositum of subfields). Suppose we have a field L and two subfields $K_1 \subseteq L$ and $K_2 \subseteq L$. Then, the compositum of K_1 and K_2 in L is the smallest subfield of L containing K_1 and K_2. We denote the compostium by $K_1 K_2$.

In fact, the compositum always exists;

the compositum of $K_1 = F(\alpha_1, \ldots, \alpha_n)$ and $K_2 = F(\beta_1, \ldots, \beta_m)$ is $K_1 K_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, _m)$.

Example 7.5. The compositum of $\mathbb{Q}\left(\sqrt{2}\right)$ and $\mathbb{Q}(\sqrt{3})$ in $\mathbb{R}$ is $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$.

Proposition 7.3. Suppose $F \subseteq L \subseteq M$, where $F \subseteq M$ is Galois. Then, the compositum of all conjugate fields of L in M is the Galois closure of $F \subseteq L$.

Lemma 7.1. The following hold:

(a) If $F \subseteq L$ and $L \subseteq M$, then so is $F \subseteq M$

(b) If $F \subseteq K_1 \subseteq L$ and $F \subseteq K_2 \subseteq L$ such that $F \subseteq K_1$ is radical, then $K_2 \subseteq K_1 K_2$ is radical

(c) If $F \subseteq K_1 \subseteq L$ and $F \subseteq K_2 \subseteq L$ such that $F \subseteq K_1$ and $F \subseteq K_2$ are radical, then $F \subseteq K_1 K_2$ is radical

Theorem 7.4. If an extension $F \subseteq L$ is separable and radical, then its Galois closure is radical.

Corollary 7.1. If a finite extension $F \subseteq L$ of characteristic 0 is solvable, then so is its Galois closure.

7.3. *Solvable Groups and Solvable Extensions*

When is a finite extension $F \subseteq L$ solvable? Because of subtleties that can occur in characteristic p, we will make the following simplifying assumption:

all fields appearing in this section will have characteristic 0.

Given a positive integer m and a field L of characteristic 0, consider the splitting field of $x^m - 1$ over L. This polynomial has m distinct roots in its splitting field. These roots form a group under multiplication, which is cyclic. A generator ζ of this group has the following two properties:

(a) The m distinct roots of $x^m - 1$ are $1, \zeta, \ldots, \zeta^{m-1}$

(b) The splitting field of $x^{-}1$ over L is $L\left(1, \zeta, \ldots, \zeta^{m-1}\right) = L(\zeta)$

We call ζ a primitive m^{th} root of unity in this situation. It is known that

$$L \subseteq L(\zeta) \text{ is Galois} \quad \text{and} \quad \operatorname{Gal}\left(L(\zeta)/L\right) \text{ is Abelian.}$$

To prove this, note that $L \subseteq L(\zeta)$ is Galois since $L(\zeta)$ is the splitting field of the separable polynomial $x^m - 1 \in L[x]$. Now, suppose $\sigma, \tau \in \operatorname{Gal}\left(L(\zeta)/L\right)$. Then, σ, τ are determined by their values on ζ. Since the roots of $x^m - 1$ are $1, \zeta, \ldots, \zeta^{m-1}$, it follows that

$$\sigma(\zeta) = \zeta^i \text{ and } \tau(\zeta) = \zeta^j \quad \text{for } i, j \in \mathbb{Z}.$$

As such,

$$\sigma\tau(\zeta) = \sigma\left(\zeta^j\right) = (\sigma(\zeta))^j = \left(\zeta^i\right)^j = \zeta^{ij}.$$

A similar computation yields $\tau\sigma(\zeta) = \zeta^{ij}$. Since $\sigma\tau = \tau\sigma$ are uniquely determined by their values on ζ, then $\sigma\tau = \tau\sigma$, which implies $\operatorname{Gal}\left(L(\zeta)/L\right)$ is Abelian.

Given a Galois extension $F \subseteq L$ and a primitive m^{th} root of unity ζ, we obtain the following extension:

$$\begin{tikzcd}
 & L(\zeta) & \\
L \arrow[ur] & & F(\zeta) \arrow[ul] \\
 & F \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

We can relate the solvability of the various Galois groups as follows:

Lemma 7.2. Let $F \subseteq L$ be a Galois extension and ζ is a primitive m^{th} root of unity. Then, $F \subseteq L(\zeta)$ and $F(\zeta) \subseteq L(\zeta)$ are also Galois, and

$$\begin{aligned}
\operatorname{Gal}(L/F) \text{ is solvable} \quad & \text{if and only if} \quad \operatorname{Gal}\left(L(\zeta)/F\right) \text{ is solvable} \\
& \text{if and only if} \quad \operatorname{Gal}\left(L(\zeta)/F(\zeta)\right) \text{ is solvable}
\end{aligned}$$

The following result will play a crucial role in our analysis of solvable extensions.

Lemma 7.3. Suppose $K \subseteq M$ is a Galois extension with $\operatorname{Gal}(M/K) \cong \mathbb{Z}/p\mathbb{Z}$, where p is prime. If K contains a primitive p^{th} root of unity ζ, then there exists $\alpha \in M$ such that $M = K(\alpha)$ and $\alpha^p \in K$.

Previously, we mentioned that if $F \subseteq L$ is solvable, then we can find an extension $L \subseteq M$ such that $F \subseteq M$ is Galois and solvable. For an arbitrary Galois extension, the wonderful fact is that the Galois group determines whether or not the extension is solvable. The following theorem due to Galois is one of the most important applications of Galois theory.

Theorem 7.5. Let $F \subseteq L$ be a Galois extension. Then,

$$F \subseteq L \text{ is a solvable extension} \quad \text{if and only if} \quad \text{Gal}\,(L/F) \text{ is a solvable group.}$$

7.4. *A Word on Simple Groups and the Jordan–Hölder Theorem*

Here is the key definition of this section.

Definition 7.5 (simple group). A group G is simple if and only if its normal subgroups are $\{e\}$ and G.

Some simple groups are easy to find.

Example 7.6. If p is prime, then Lagrange's theorem implies that the cyclic group $\mathbb{Z}/p\mathbb{Z}$ is simple. In fact, these are the only non-trivial Abelian finite simple groups.

Here is a more interesting example.

Example 7.7. The alternating group A_n is simple for $n \geq 5$.

We next observe that non-Abelian finite simple groups are not solvable.

Lemma 7.4. Let G be a non-Abelian finite simple group. Then, G is not solvable.

Proof. Suppose on the contrary that G is solvable. Then, we can find a normal subgroup $G_1 \trianglelefteq G$ such that $[G : G_1]$ is prime. Since G is simple, we must have $G_1 = \{e\}$, which implies $G_1 \neq G$. By Lagrange's theorem, we have

$$|G| = [G : G_1]\,|G_1| = [G : G_1]\,|\{e\}| = [G : G_1]\,,$$

which implies G has prime order. Recall that in MA2202, if G is of prime order, then it must be cyclic and hence, Abelian. However, we mentioned that G is non-Abelian, which is a contradiction. □

As such, we infer that the following theorem hold:

Theorem 7.6. A_n and S_n are solvable if and only if $n \leq 4$.

We will only prove special cases of Theorem 7.6 in Theorems 7.7 and 7.8, i.e. show that S_3 and S_4 are solvable.

Theorem 7.7. S_3 is solvable.

Proof. Note that $\{e\} \subseteq A_3 \subseteq S_3$. We will justify that $A_3 \trianglelefteq S_3$, and S_3/A_3 is Abelian. The first property is obvious; for the second property, we use the first isomorphism theorem to indirectly derive a stronger result. Consider the homomorphism $\phi : S_3 \to \mathbb{Z}_2$, where

$$\phi((1)) = 0 \equiv 0 \pmod 2 \text{ and } \phi((2\,3)) = 1 \equiv 1 \pmod 2.$$

So, We leave it to the reader to check for the four remaining permutations. $\ker\phi$ consists of elements in S_3 that map to the identity in $\mathbb{Z}_2$, which is 0. So, we need to find the permutations in S_3 that are mapped to 0 modulo 2 (i.e. even permutations), which are $(1), (1\,2\,3)$ and $(1\,3\,2)$. These are even permutations, so it is clear that $\ker\phi = A_3$. Lastly, recall that $\mathbb{Z}_2$ is the group of integers under addition modulo 2, which is obviously Abelian. We conclude that S_3 is solvable. □

Theorem 7.8. S_4 is solvable.

Proof. We see that $V \trianglelefteq A_4$ and $A_4 \trianglelefteq S_4$. Also, it is obvious that $\{e\} \trianglelefteq V$. Thus, $|S_4/|A_4| = 24/12 = 2$, which is prime. By Lagrange's theorem, $|S_4/|A_4|$ is cyclic and thus Abelian. Similarly, $|A_4/V| = 12/4 = 3$ so A_4/V is cyclic and thus, Abelian. So, S_4 is solvable. □

In fact, it follows from Theorems 7.7 and 7.8 that A_3 and A_4 are also solvable. For later purposes, we determine the normal subgroups of S_n.

Proposition 7.4. If $n \geq 5$ and $H \trianglelefteq S_n$, then either

$$H = \{e\} \quad \text{or} \quad H = A_n \quad \text{or} \quad H = S_n.$$

The relationship between simple groups and solvable groups is more interesting than just simply mentioning that every non-Abelian finite simple group G is not solvable (Lemma 7.4). The key observation is that groups are built out of simple groups by means of what are called composition series.

Recall Definition 7.1 where we mentioned that a group G is solvable if we can find subgroups

$$\{e\} = G_n \subseteq G_{n-1} \subseteq \ldots \subseteq G_1 \subseteq G_0 = G$$

such that $G_i \trianglelefteq G_{i-1}$ and $[G_{i-1} : G_i]$ is prime for all $1 \leq i \leq n$. This implies that the quotient G_{i-1}/G_i is simple.

More generally, if G is a finite group, then a composition series of G comprises subgroups $G_n, G_{n-1} \ldots, G_1, G_0$ such that $G_i \trianglelefteq G_{i-1}$ and the quotient G_{i-1}/G_i is simple for all i. We call G_{i-1}/G_i the composition factors of G.

Example 7.8. Let $n \geq 5$. Since A_n is simple by Example 7.7, a composition series of S_n is

$$\{e\} \subseteq A_n \subseteq S_n.$$

The composition factors are $A_n/\{e\} \cong A_n$ and $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$.

It is straightforward that any finite group has a composition series (proven in Example 7.9). However, a given group may have more than one composition series. For example, the cyclic group

$\mathbb{Z}/6\mathbb{Z} = \langle 1 \rangle$ has the composition series

$$\{e\} \subseteq \langle 2 \rangle \subseteq \mathbb{Z}/6\mathbb{Z} \quad \text{and} \quad \{e\} \subseteq \langle 3 \rangle \subseteq \mathbb{Z}/6\mathbb{Z}.$$

The factors of the first composition series are $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$, while the factors for the second are $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$. The Jordan–Hölder theorem asserts that any two composition series of a given group have the same length and that the corresponding composition factors can be permuted so that they become isomorphic. Hence, the composition factors of a group are the simple groups from which the group is *built* (some explanation is required here but we will not explain).

Example 7.9 (Cox p. 215 Question 6)**.** Let G be a finite group.

(a) Among all normal subgroups of G different from G itself, pick one of maximal order and call it H. Prove that G/H is a simple group.

(b) Use **(a)** and induction on $|G|$ to prove that G has a composition series.

Solution.

(a) We shall argue by contradiction. Suppose there exists N such that $N \trianglelefteq G/H$. Then,

$$(aH)(nH)(aH)^{-1} \in G/H \quad \text{for all } aH \in G/H \text{ and } nH \in N.$$

Note that $aH \in G/H$ is equivalent to saying that $a \in G$. Also, the expression

$$(aH)(nH)(aH)^{-1} = \left(ana^{-1}\right)H.$$

This shows that $ana^{-1} = n$ since $N \trianglelefteq G$ by assumption. Thus,

$$Z(G) = \{n \in G : nH \in G/N\}.$$

This implies $H \subseteq N$. However, H was chosen to be the largest normal subgroup of G, which leads to a contradiction. As such, G/H is simple.

(b) Suppose $|G| = n$. Let $P(n)$ denote the proposition that G has a composition series. The base case is obviously true as the composition series only comprises the trivial group $\{e\}$.

Assume that for all $k < n$, the proposition holds. Then, for the case when $|G| = n$, let H be a normal subgroup G different from G itself, say H, where H is of maximal order. By the inductive hypothesis, H has the following composition series:

$$\{e\} = G_n \subseteq \ldots \subseteq H.$$

By **(a)**, G/H is simple, so

$$\{e\} = G_n \subseteq \ldots \subseteq H \subseteq G$$

is a composition series.

7.5. *Solving Polynomials by Radicals*

The problem of solving a polynomial equation for its zeros can be transformed into a problem regarding field extensions. At the same time, we can use the Fundamental Theorem of Galois Theory to transform a problem about field extensions into a problem about groups. This is how Galois showed that there are fifth-degree polynomials that cannot be solved by radicals.

We will assume that all fields appearing in this section will have characteristic zero. So far, our discussion of solvability by radicals has focused on field extensions. We now shift our attention to polynomials and their roots.

Definition 7.6 (solvability by radicals)**.** Let $f \in F[x]$ be non-constant with splitting field $F \subseteq L$.

(a) A root $\alpha \in L$ of f is expressible by radicals over F if α lies in some radical extension of F.

(b) The polynomial f is solvable by radicals over F if $F \subseteq L$ is a solvable extension.

Example 7.10. Let

$$\omega = e^{2\pi i/8} = \frac{\sqrt{2}}{2} + i\left(\frac{\sqrt{2}}{2}\right).$$

Then, x^8-3 splits over $\mathbb{Q}\left(\omega, \sqrt[3]{8}\right)$, where $\omega^8 \in \mathbb{Q}$ and $\left(\sqrt[3]{8}\right)^8 \in \mathbb{Q} \subseteq \mathbb{Q}(\omega)$. Thus, x^8-3 is solvable by radicals over $\mathbb{Q}$. Although the zeros of x^8-3 are written in the form $r, r\omega, r\omega^2, \ldots, r\omega^7$, where $r = \sqrt[3]{8}$, the notion of solvable by radicals is best illustrated by writing them in the form

$$\pm r, \pm ir, \pm r\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right), \pm r\left(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right).$$

In fact, we also could have considered the chain of extensions

$$\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt[3]{8}\right) \subseteq \mathbb{Q}\left(\sqrt[3]{8}, \omega\right).$$

Note that these extensions are radical since $\sqrt[3]{8}$ is the cube root of a rational number. Also, cyclotomic extensions like $\mathbb{Q}\left(e^{2\pi i/8}\right)$ are radical as the minimal polynomial of a root of unity over $\mathbb{Q}$ is reducible into factors over extensions by successive roots of unity.

By the definition of solvability by radicals (Definition 7.6), if a non-constant polynomial in $F[x]$ is solvable by radicals, then all of its roots are expressible by radicals. However, for an irreducible polynomial, it turns out that solvability by radicals is satisfied as soon as one root is expressible by radicals. Here is the precise result.

Proposition 7.5. Let $f \in F[x]$ be irreducible. Then, f is solvable by radicals over F if and only if f has a root expressible by radicals over F.

Theorem 7.9. A polynomial $f \in F[x]$ is solvable by radicals over F if and only if the Galois group of f over F is solvable.

We can apply this to polynomials of low degree as follows.

Proposition 7.6. If $f \in F[x]$ has degree $n \leq 4$, then f is solvable by radicals.

Once we get to degree 5, a different picture emerges.

Example 7.11. Consider the quintic polynomial $f = x^5 - 6x + 3$, which has S_5 as Galois group over $\mathbb{Q}$. However, S_5 is not solvable, so f is not solvable by radicals over $\mathbb{Q}$. Furthermore, f is irreducible by Eisenstein's criterion (set $p = 3$) so it follows that no root of f is expressible by radicals over $\mathbb{Q}$.

This example requires that we revise how we think about the roots of a polynomial. Most students come into a course on Galois theory thinking that the roots of a polynomial $f \in \mathbb{Q}[x]$ are numbers like

$$\sqrt{2}+\sqrt{3} \quad \sqrt{2+\sqrt{2}} \quad \sqrt[7]{12+7i} \quad \ldots$$

Historically, the word 'root' came to refer to a solution of $f(x) = 0$ because of the intuition that roots are built from radicals. However, we saw in Example 7.11 that this intuition is wrong — roots of polynomials are intrinsically more complicated than just radicals.

Theorem 7.10. Let H be a subgroup of S_5 that contains a 5-cycle and a 2-cycle. Then, $H = S_5$.

Proof. Let

$$\sigma = (12345) \quad \text{and} \quad \tau = (1,2).$$

Then,

$$\begin{aligned} \sigma\tau\sigma^{-1} &= (12345)(12)(54321) = (23) \\ \sigma^2\tau\sigma^{-2} &= (34) \\ \sigma^3\tau\sigma^{-3} &= (45) \\ \sigma^4\tau\sigma^{-4} &= (51) \end{aligned}$$

Since every permutation is a product of transpositions and every transposition can be generated by σ and τ, then the result follows. □

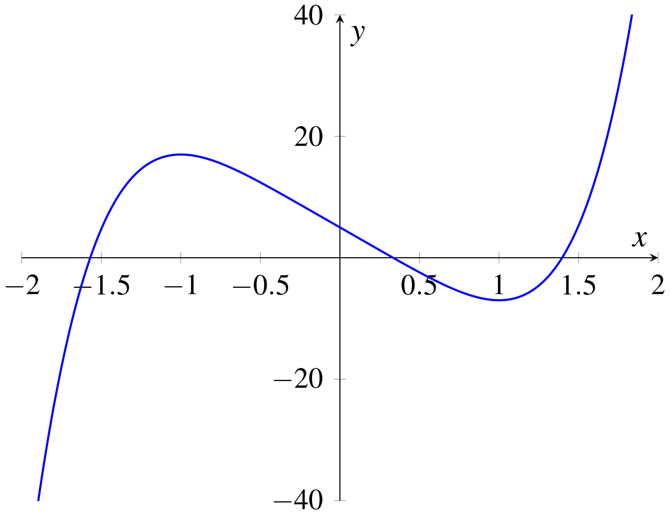
Here is another example of a polynomial $\in \mathbb{Z}[x]$ but not solvable by radicals over $\mathbb{Q}$.

Example 7.12. Let

$$g(x) = 3x^5 - 15x + 5.$$

By Eisenstein's criterion, choosing $p = 5$ implies $g(x)$ is irreducible over $\mathbb{Q}$.

Using techniques in Real Analysis, $g(x)$ is continuous and $g(-2) = -61$ and $g(-1) = 17$. By the intermediate value theorem, there exists $c \in (-2,-1)$ such that $g(c) = 0$. A similar argument shows that $g(x)$ has real zeros between 0 and 1 and between 1 and 2.



Each of these zeros has multiplicity 1. Furthermore, $g(x)$ has no more than three real zeros because Rolle's theorem asserts that between each pair of real zeros of $g(x)$, there must be a zero of $g'(x) = 15x^4 - 15$. So, for $g(x)$ to have four real zeros, $g'(x)$ would need to have three real zeros, but it does not. Thus, the two other zeros of $g(x)$ are complex, say $a+bi$ and $a-bi$ (conjugate roots occur by the conjugate root theorem).

Denote the five zeros of $g(x)$ by $a_1,\ldots,a_5$. Since any automorphism of $K = \mathbb{Q}(a_1,\ldots,a_5)$ is completely determined by its action on the a_i's and must permute the a_i's, then $\mathrm{Gal}(K/\mathbb{Q}) \leq S_5$. Since a_1 is a zero of an irreducible polynomial of degree 5 over $\mathbb{Q}$, then $[\mathbb{Q}(a_1):\mathbb{Q}] = 5$, so by the tower theorem, 5 divides $[K:\mathbb{Q}]$. **(i)** of The Fundamental Theorem of Galois Theory (Theorem 6.5) asserts that $5 \mid |\mathrm{Gal}(K/\mathbb{Q})|$. By Lagrange's theorem, $\mathrm{Gal}(K/\mathbb{Q})$ has an element of order 5.

Since the only elements of order 5 are the 5-cyles, then $\mathrm{Gal}(K/\mathbb{Q})$ contains a 5-cycle. Next, consider the map

$$\sigma : \mathbb{C} \to \mathbb{C} \quad \text{where} \quad \sigma : a+bi \mapsto a-bi \text{ (essentially conjugation map).}$$

σ fixes the three real zeros and interchanges the two complex zeros of $g(x)$ so $\mathrm{Gal}(K/\mathbb{Q})$ contains a 2-cycle. However, by Theorem 7.10, the only subgroup of S_5 that contains both a 5-cycle and a 2-cycle is S_5. So, $\mathrm{Gal}(K/\mathbb{Q}) \cong S_5$. Since S_5 is not solvable, then we have exhibited a polynomial of degree five that is not solvable by radicals.

8. Cyclotomic Extensions

8.1. *Cyclotomic Polynomials*

In this chapter, we will explore the Galois theory of cyclotomic extensions, which are extensions of the form $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{2\pi i/n}$. This involves the study of cyclotomic polynomials. In the next chapter, we will apply such results to determine which regular polygons are constructible by straightedge and compass.

As a prelude, note that if p is prime, then

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 \quad \text{is} \quad \text{the minimal polynomial of } \zeta_p = e^{2\pi i/p} \text{ over } \mathbb{Q}.$$

Now, we will describe the minimal polynomial of $\zeta_n = e^{2\pi i/n}$ over $\mathbb{Q}$, where n is now an arbitrary integer ≥ 1. We will also compute the Galois group $\text{Gal}(L/Q)$, where $L = \mathbb{Q}(\zeta_n)$. One would need some pre-requisite on Number Theory.

Definition 8.1 (Euler totient function). Let $n \in \mathbb{Z}^+$. Define the Euler totient function $\phi(n)$ to be the number of integers i such that $0 \leq i < n$ and $\gcd(i,n) = 1$.

We can interpret $\phi(n)$ in terms of the ring $\mathbb{Z}/n\mathbb{Z}$. The invertible elements of this ring form the set

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[i] \in \mathbb{Z}/n\mathbb{Z} : [i][j] = 1 \text{ for some } j \in \mathbb{Z}/n\mathbb{Z}\}.$$

One sees that $(\mathbb{Z}/n\mathbb{Z})^*$ is a group under multiplication. In fact, the group is of order $\phi(n)$ (Example 8.1).

Example 8.1 (Cox p. 236 Question 1). Prove that

$$\text{a congruence class } [i] \in \mathbb{Z}/n\mathbb{Z} \text{ has a multiplicative inverse} \quad \text{if and only if} \quad \gcd(i,n) = 1.$$

Conclude that $(\mathbb{Z}/n\mathbb{Z})^*$ has order $\phi(n)$. Be sure you understand what happens when $n = 1$.

Solution. For the forward direction, suppose $[i] \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse, say $[j]$. This means that $ij \equiv 1 \pmod{n}$. In other words, there exists $k \in \mathbb{Z}$ such that $ij - kn = 1$. By the converse of Bézout's lemma, $\gcd(i,n) = 1$.

As for the reverse direction, we use Bézout's lemma to deduce that

$$\text{there exist } x, y \in \mathbb{Z} \quad \text{such that} \quad xi + yn = 1.$$

Considering both sides of the equation modulo n, we have $xi \equiv 1 \pmod{n}$, so it follows that $[x]$ is the multiplicative inverse of $[i]$.

Since $\phi(n)$ counts the number of $i < n$ such that $\gcd(i,n) = 1$, it follows that $\left|(\mathbb{Z}/n\mathbb{Z})^*\right| = \phi(n)$.

When $n = 1$, the ring $\mathbb{Z}/1\mathbb{Z}$ contains only one element, namely $[0]$. The congruence class $[0]$ does not have a multiplicative inverse, as there is no j such that $0 \cdot j \equiv 1 \pmod 1$. Hence, the group $(\mathbb{Z}/1\mathbb{Z})^*$ is the trivial group, and its order is 0, which is consistent with $\phi(1) = 1$. □

Our first lemma gives the basic properties of the ϕ-function (should have been covered in MA3265).

Lemma 8.1. Let ϕ denote the Euler totient function.

(a) Multiplicativity: If $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$

(b) If $n > 1$ is an integer, then

$$\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$$

Lemma 8.2 (Fermat's little theorem)**.** If p is prime, then $a^p \equiv a \pmod p$ for all $a \in \mathbb{Z}$.

Our next task is to define the cyclotomic polynomial $\Phi_n(x)$ for $n \geq 1$; in fact, it has integer coefficients. We begin with the factorisation

$$x^n - 1 = \prod_{0 \leq i < n}\left(x - \zeta_n^i\right).$$

Then, we define the n^{th} cyclotomic polynomial $\Phi_n(x)$ as follows:

Definition 8.2 (cyclotomic polynomial)**.** The n^{th} cyclotomic polynomial $\Phi_n(x)$ is defined to be the product

$$\Phi_n(x) = \prod_{\substack{0 \leq i < n \\ \gcd(i,n)=1}}\left(x - \zeta_n^i\right).$$

We see that the roots of $\Phi_n(x)$ are ζ_n^i for those $0 \leq i < n$ relatively prime to n. It follows that the degree of the polynomial $\Phi_n(x)$ is $\phi(n)$. As such,

$$\phi(n) = \deg(\Phi_n(x)) = \left|(\mathbb{Z}/n\mathbb{Z})^*\right|.$$

This link between $\Phi_n(x)$ and $(\mathbb{Z}/n\mathbb{Z})^*$ will be used to determine the Galois group $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Previously, we defined a root of $x^n - 1$ to be a primitive n^{th} root of unity if its powers give all roots of $x^n - 1$ (recall the concept of the generator of a cyclic group in MA2202). In our situation, the primitive n^{th} roots of unity are ζ_n^i for $0 \leq i < n$ and $\gcd(i,n) = 1$. Thus,

$$\text{the roots of } \Phi_n(x) \quad \text{are} \quad \text{the primitive } n^{\text{th}} \text{ roots of unity in } \mathbb{C}.$$

We now provide some examples of cyclotomic polynomials.

Example 8.2. When $n = 2$, the only primitive square root of unity is -1 so that $\Phi_2(x) = x + 1$; when $n = 4$, the primitive fourth roots of unity are i and $i^3 = -1$ so that

$$\Phi_4(x) = (x - i)(x + i) = x^2 + 1.$$

Since $\Phi - 1(x) = x - 1$, we obtain the factorisation

$$x^4 - 1 = (x - 1)(x + 1)\left(x^2 + 1\right) = \Phi_1(x)\Phi_2(x)\Phi_4(x).$$

In general, $x^n - 1$ has a similar factorisation.

Example 8.3 (p^{th} cyclotomic polynomial)**.** Let p be a prime. Since $1, \ldots, p - 1$ are relatively prime to p, or equivalently $\gcd(i, p) = 1$ for all $i < p$, it follows that

$$\Phi_p(x) = \prod_{i=1}^{p-1}\left(x - \zeta_p^i\right) = \frac{x^p - 1}{x - 1}.$$

Proposition 8.1. $\Phi_n(x)$ is a monic polynomial with integer coefficients and has degree $\phi(n)$. Moreover, these polynomials satisfy the identity

$$x^n - 1 = \prod_{d|n}\Phi_d(x).$$

Example 8.4. The identity

$$x^p - 1 = \Phi_1(x)\Phi_p(x)$$

seems like a *boring* application of Proposition 8.1. To spice things up a little, we have

$$x^{p^2} - 1 = \Phi_1(x)\Phi_p(x)\Phi_{p^2}(x).$$

It follows that $x^{p^2} - 1 = (x^p - 1)\Phi_{p^2}(x)$.

Remark 8.1. In the examples of cyclotomic polynomials given so far, the coefficients are always 0 or ± 1. This is true for all $n < 105$, i.e. the pattern breaks for $n \geq 105$.

We are now in position to discuss the Galois group of a cyclotomic extension. The first step in computing $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is to prove that $\Phi_n(x)$. We omit the proof here.

Theorem 8.1. The cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

Corollary 8.1. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$

This makes it easy to compute the Galois group of a cyclotomic extension.

Theorem 8.2. Let $L = \mathbb{Q}(\zeta_n)$. There exists an isomorphism

$$\operatorname{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^* \quad \text{such that} \quad \sigma \mapsto [\ell]$$

if and only if $\sigma(\zeta_n) = \zeta_n^\ell$.

Example 8.5. Consider the field $\mathbb{Q}(\zeta_5)$, where $\zeta_5 = e^{2\pi i/5}$. The roots of the polynomial $x^5 - 1$ are $\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4, 1$. Excluding 1, the other four roots form a cyclic group under multiplication. An element $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ must permute the roots of $x^5 - 1$ in a way that preserves their algebraic structure. In particular, $\sigma(\zeta_5)$ must be another 5th root of unity, say ζ_5^ℓ, where $\gcd(\ell, 5) = 1$. In fact, there are precisely four choices for ℓ since 5 is prime.

On the other hand, the group $(\mathbb{Z}/5\mathbb{Z})^*$ consists of the integers $1, 2, 3, 4$ modulo 5 since these integers are coprime to 5 (implicitly mentioned earlier). Under multiplication modulo 5, they form a group. Each $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ corresponds to an element $[\ell]$ in $(\mathbb{Z}/5\mathbb{Z})^*$. We can have either of the following:

$$\begin{aligned}
[\ell] &= 1 \quad \text{which corresponds to} \quad \sigma(\zeta_5) = \zeta_5 \text{ (identity map)} \\
[\ell] &= 2 \quad \text{which corresponds to} \quad \sigma(\zeta_5) = \zeta_5^2 \\
[\ell] &= 3 \quad \text{which corresponds to} \quad \sigma(\zeta_5) = \zeta_5^3 \\
[\ell] &= 4 \quad \text{which corresponds to} \quad \sigma(\zeta_5) = \zeta_5^4
\end{aligned}$$

The identity map case is quite boring. We first give an example of how the $[\ell] = 3$ case works. For any root ζ_5^k, where $1 \le k \le 4$, we must be able to obtain it from the map $\sigma(\zeta_5) = \zeta_5^3$. We have

$$\sigma(\zeta_5^2) = \zeta_5 \quad \text{and} \quad \sigma(\zeta_5^3) = \zeta_5^4 \quad \text{and} \quad \sigma(\zeta_5^4) = \zeta_5^2.$$

See Figure 1 for a visual representation of how σ acts on the roots.

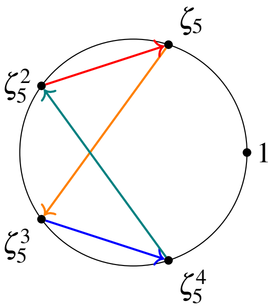


Figure 1: Action of σ with $[\ell] = 3$

We then consider the $[\ell] = 2$ case. Again, we have $\sigma(\zeta_5) = \zeta_5^2$, so

$$\sigma(\zeta_5^2) = \zeta_5^4 \quad \text{and} \quad \sigma(\zeta_5^3) = \zeta_5 \quad \text{and} \quad \sigma(\zeta_5^4) = \zeta_5^3.$$

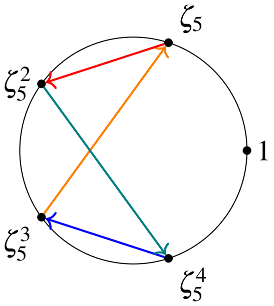


Figure 2: Action of σ with $[\ell] = 2$

See Figure 2 for a visual representation of how σ acts on the roots.

Lastly, we consider the $[\ell] = 4$ case. Again, we have $\sigma(\zeta_5) = \zeta_5^4$, so

$$\sigma\left(\zeta_5^2\right) = \zeta_5^3 \quad \text{and} \quad \sigma\left(\zeta_5^3\right) = \zeta_5^2 \quad \text{and} \quad \sigma\left(\zeta_5^4\right) = \zeta_5.$$

See Figure 3 for a visual representation of how σ acts on the roots.

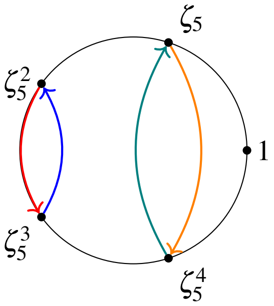


Figure 3: Action of σ with $[\ell] = 4$

9. Geometric Constructions

9.1. *Constructible Numbers*

A straightedge is an unmarked ruler, whereas a compass is a device used to draw circular arcs. Using a straightedge and a compass, we can produce points on a plane starting with two given points 0 and 1. We now carefully describe the points, lines, and circles that we can construct using straightedge and compass starting from 0 and 1.

Postulate 9.1 (geometric construction postulates). C1 and C2 represent constructive postulates that describe basic allowable constructions in geometry; P1, P2, and P3 are often called intersection principles or incidence postulates. They allow the identification of points that satisfy specific conditions.

- **C1:** From two points α and β, we can construct a line ℓ that passes through α and β
- **C2:** Given three points α, β, γ, we can draw a circle C with centre γ whose radius is the distance between α and β
- **P1:** The point of intersection of distinct lines ℓ_1 and ℓ_2
- **P2:** The points of intersection of a line ℓ and a circle
- **P3:** The points of intersection of two circles

ℓ
α
β
γ
C
$r = |\alpha - \beta|$

Figure 4: **C1:** line through two points (left); **C2:** circle with centre and radius (right)

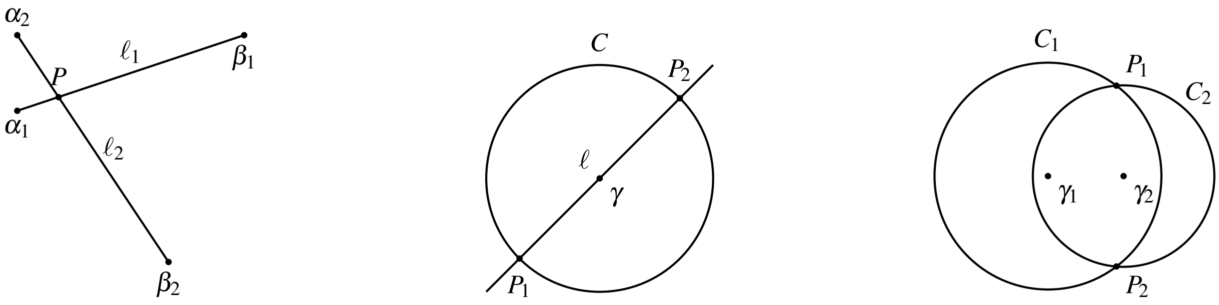


Figure 5: **P1:** intersection of two lines (left); **P2:** intersection of a line and a circle (middle); **P3:** intersection of two circles (right)

We identify the plane as the geometric representation of $\mathbb{C}$. Constructing a point on the plane will mean constructing a complex number. As mentioned, we will start our construction from 0 and 1.

Definition 9.1 (constructible number). We say that $\alpha \in \mathbb{C}$ is constructible if there exists

$$\text{a finite sequence of straightedge and compass constructions} \quad \text{using} \quad C_1, C_2, P_1, P_2, P_3$$

that begins with 0 and 1 and ends with α.

We provide some examples of constructible numbers.

Example 9.1 (constructing $\mathbb{Z}$). From 0 and 1, we use C1 to construct a line passing through 0 and 1. This line can be extended indefinitely, so we obtain the x-axis. By considering C2, we construct the circle of radius 1 centred at 1. This circle intersects the numbers 0 and 2, or to be explicit, $(0,0)$ and $(2,0)$. By P2, 2 is constructible.

We have constructed $0,1,2$ thus far. Iterating this shows that every $n \in \mathbb{Z}$ is constructible.

Example 9.2 (y-axis is constructible; Dummit and Foote p. 267 Question 1). In Example 9.1, we constructed the x-axis. In a similar way, show that the y-axis is constructible. For each step in your construction, be sure to say which of C1, C2, P1, P2 and P3 you are using.

Solution. From Example 9.1, it follows that $-1,0,1$ are constructible. By C2, we can construct the following circles:

$$\text{the one centred at } -1 \text{ with radius } 2 \quad \text{and} \quad \text{the one centred at } 1 \text{ with radius } 2.$$

By simple high school geometry, we obtain the intersection points of these two circles by P3, which are $\pm i\sqrt{3}$. By C1, we can construct a line that passes through $i\sqrt{3}$ and $-i\sqrt{3}$. Iterating this (similar to Example 9.1) shows that the y-axis is constructible. □

Example 9.3 ($i \in \mathbb{C}$ is constructible). In Example 9.2, we showed that the y-axis is constructible. Using C2, we can draw a circle of radius 1 centred at 0. These intersect at $\pm i$, which shows that $i \in \mathbb{C}$ is constructible.

Example 9.4 (ζ_n is constructible). Suppose we can construct a regular n-gon somewhere in the place. Using two consecutive vertices and the centre of the n-gon, one is able to construct an isosceles triangle with the angle at the centre being $\theta = 2\pi/n$ (Figure 6).

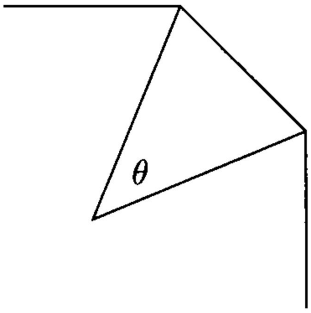


Figure 6

The constructed triangle can be *copied* such that the angle θ is oriented anticlockwise from the positive part of the x-axis (Figure 7). Intersecting this with the unit circle shows that the n^{th} root of unity $\zeta_n = e^{2\pi i/n}$ is constructible. In fact, this process can be reversed.

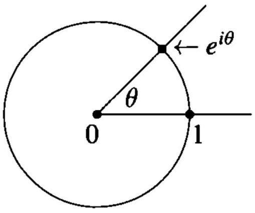


Figure 7

We conclude that

ζ_n is constructible if and only if a regular n-gon can be constructed by straightedge and compass.

We will discuss a beautiful result in Theorem 9.5, known as the Gauss-Wantzel theorem, which provides a criterion to determine those n's for which this is possible.

The set of constructible numbers $\mathscr{C}$ has the following properties:

Theorem 9.1. Let

$$\mathscr{C} = \{a \in \mathbb{C} : \alpha \text{ is constructible}\} \quad \text{is a subfield of } \mathbb{C}.$$

(a) Let $\alpha = a + bi \in \mathbb{C}$, where $a, b \in \mathbb{R}$. Then,

$$\alpha \in \mathscr{C} \quad \text{if and only if} \quad a, b \in \mathscr{C}$$

(b) $\alpha \in \mathscr{C}$ implies $\sqrt{\alpha} \in \mathscr{C}$

Example 9.5. $\zeta_5 = e^{2\pi i/5}$ is given by the formula

$$\zeta_5 = \frac{-1+\sqrt{5}}{4} + \frac{i}{2}\sqrt{\frac{5+\sqrt{5}}{2}}.$$

Since $\mathscr{C}$ is closed under the operation of taking square roots, it follows easily that ζ_5 is constructible. Consequently, a regular polygon can be constructed by straightedge and compass.

We call $\mathscr{C}$ the field of constructible numbers. We next study the structure of $\mathscr{C}$.

Theorem 9.2. Let $\alpha \in \mathbb{C}$. Then, $\alpha \in \mathscr{C}$ if and only if there exists subfields

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_{n-1} \subseteq F_n \subseteq \mathbb{C}$$

such that $\alpha \in F_n$ and $[F_i : F_{i-1}] = 2$ for all $1 \leq i \leq n$.

Essentially, a vague description of the reverse direction of Theorem 9.2 is as follows: say F_i is a quadratic extension of F_{i-1} since the degree of each field extension is 2. Then, by constructing the aforementioned chain with $\alpha \in \mathbb{C}$, it follows that $\alpha \in \mathscr{C}$, i.e. α is constructible.

Corollary 9.1. $\mathscr{C}$ is the smallest subfield of $\mathbb{C}$ that is closed under the operation of taking square roots.

Corollary 9.2 (constructible number implies algebraic over $\mathbb{Q}$)**.** If $\alpha \in \mathscr{C}$, then

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m \quad \text{for some } m \geq 0.$$

Thus, every constructible number is algebraic over $\mathbb{Q}$, and the degree of its minimal polynomial over $\mathbb{Q}$ is a power of 2.

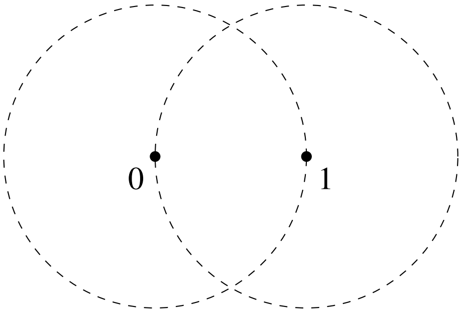
Example 9.6 (Cox p. 268 Question 5)**.** In this exercise, you will give two proofs that $\zeta_3 = e^{2\pi i/3}$ is constructible.

(a) Give a direct geometric construction of ζ_3 with each step justified by citing C1, C2, P1, P2, or P3.

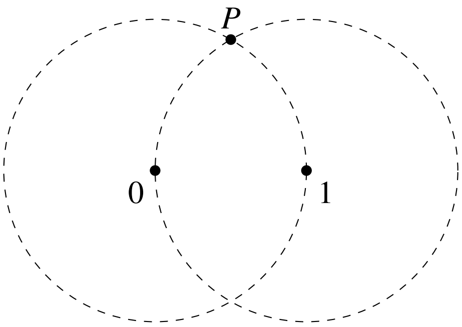
(b) Use Theorem 9.2 to show that ζ_3 is constructible.

Solution.

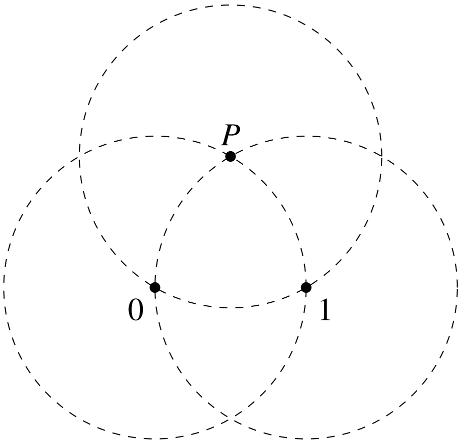
(a) Consider the points 0 and 1. Using C2, we can construct a circle of radius 1 centred at 0, and another circle of radius 1 centred at 1.



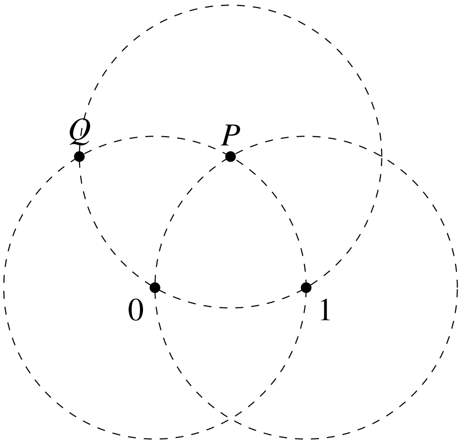
Using P3, define P to be the point of intersection of the two circles.



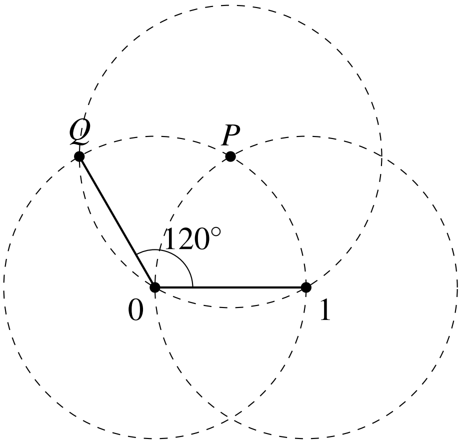
Use C2 to construct a third circle of radius 1 centred at P. The reason why this circle is of radius 1 is because the distance from 0 to P is the same as the distance from 1 to P, which is 1.



Using P3, define Q to be the point of intersection with one of the first two circles and the newest circle.



The smaller angle formed by the sides $0Q$ and 01 is 120°.



(b) The extension $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_3)$ is of degree 2 since ζ_3 satisfies the equation x^2+x+1, which is of degree 2. By Theorem 9.2, the result follows. □

Example 9.7 (Cox p. 273 Question 4)**.** Prove that

$$(\zeta_n)^{n/m} = \zeta_m \quad \text{when } m \mid n \text{ and } m > 0.$$

Use this to conclude that if ζ_n is constructible and $m \mid n$, where $m > 0$, then ζ_m is constructible.

Solution. Suppose $m \mid n$, where $m > 0$. Then, there exists $d \in \mathbb{Z}$ such that $n = dm$. So,

$$(\zeta_n)^{n/m} = \zeta_{dm}^d = \left(e^{2\pi i/dm}\right)^d = e^{2\pi i/m} = \zeta_m.$$

As such, ζ_m lies in the same field as ζ_n or a subfield of it. Recall that $\mathscr{C}$ is a subfield of $\mathbb{C}$ (Corollary 9.1). Since ζ_n is constructible, then ζ_m is constructible. □

Some of the most famous problems in Greek geometry are as follows:

trisection of the angle and duplication of the cube and squaring the circle

Example 9.8 (trisection of the angle). We know that every angle can be bisected using straightedge and compass. However, this is not true for trisections, i.e. there exist angles that cannot be trisected by straightedge and compass. For example, say that we can trisect a 120° angle. Since we can construct a 120° angle from 0 and 1 by straightedge and compass (Example 9.6), a trisection of this angle would imply that we could construct a 40° angle from 0 and 1 by straightedge and compass. Intersecting this with the unit circle centred at the origin, it follows that ζ_9 is a constructible number since $40^\circ = 2\pi/9$.

We have the factorisation

$$x^9 - 1 = \Phi_1(x)\,\Phi_3(x)\,\Phi_9(x) = (x-1)\left(x^2+x+1\right)\left(x^6+x^3+1\right).$$

but one checks that $x^6 + x^3 + 1$ is the minimal polynomial of ζ_9. Since the degree of this polynomial is not a power of 2, it follows that ζ_9 is not constructible. As such, we cannot trisect 120° using straightedge and compass.

Example 9.9 (Cox p. 268 Question 6). Show that it is impossible to trisect a 60° angle by straightedge and compass.

Solution. Suppose on the contrary that it is possible to trisect. Then, we can construct a 20° angle from 0 and 1 by straightedge and compass. Similar to Example 9.8, intersecting this with the unit circle centred at the origin, it follows that ζ_{18} is a constructible number since $20^\circ = 2\pi/18$.

We have the factorisation

$$x^{18} - 1 = \left(x^9+1\right)\left(x^6+x^3+1\right)\left(x^2+x+1\right)(x-1)$$

It is easy to check that $x^6 - x^3 + 1$ is the minimal polynomial of ζ_{18}. Since the degree of this polynomial is not a power of 2, it follows that ζ_{18} is not constructible. The result follows. □

Example 9.10 (duplication of the cube). This is also known as the Delian problem. Say we are given a cube and we wish to construct another with exactly twice the volume. We can pick our units of measurement so that the given cube has edges of length 1. In these units, the volume is also 1, which means that we need to construct a cube of volume 2. It follows that if we could duplicate the cube, then we could construct a number s such that $s^3 = 2$. Equivalently, $s = \sqrt[3]{2}$. Furthermore, since the cube has edge length 1, we can assume that the construction begins with 0 and 1.

If duplication of the cube by straightegde and compass holds, then it would imply that $s = \sqrt[3]{2}$ is constructible. We will justify that this is not true by contraposition. Recall that $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$, for which the polynomial is of degree 3. So, $\sqrt[3]{2}$ is not constructible. We conclude that we cannot duplicate the cube by straightedge and compass.

Example 9.11 (squaring the circle)**.** This involves constructing a square whose area is equal to that of a given circle. Suppose the given circle has radius 1. Then, the circle has area π. Since a square of area π has side $\sqrt{\pi}$, it follows that if we could square the circle, then we could construct $\sqrt{\pi}$. Furthermore, since the circle has radius 1, we can assume that the construction begins with 0 and 1. It follows that squaring the circle by straightedge and compass would imply that $\sqrt{\pi}$ is constructible.

Recall that $\mathscr{C}$ is a field, so by a closure property, the constructibility of $\sqrt{\pi}$ would imply that its square, π, is also constructible. Recall Corollary 9.2. As π is claimed to be constructible, then it must be algebraic over $\mathbb{Q}$. However, a known result by Lindemann and Weierstrass (Lindemann-Weierstrass theorem) asserts that π is transcendental over $\mathbb{Q}$, resulting in a contradiction!

One would ask whether the converse of Corollary 9.2 is true, i.e. is it true that if $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ and the degree of its minimal polynomial is a power of 2, then α is constructible? Well, we must have the degree of the splitting field L over $\mathbb{Q}$ to be some power of 2. We will state this result now.

Theorem 9.3. Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$, and let $\mathbb{Q} \subseteq L$ be the splitting field of the minimal polynomial of α over $\mathbb{Q}$. Then, α is constructible if and only if $[L : \mathbb{Q}]$ is a power of 2.

We continue our discussion with the quadratrix of Hippias. On pages 268 and 269 of Cox's textbook, Question 10 (of what we will be discussing) is left as an exercise for the reader. We will use this curve to

square the circle and trisect the angle.

The quadratrix is defined to be the curve

$$y = x\cot\left(\frac{\pi x}{2}\right) \quad \text{for } 0 < x \leq 1 \text{ (Figure 8).}$$

A simple result in Calculus shows that

$$\frac{2}{\pi} = \lim_{x \to 0^+} x\cot\left(\frac{\pi x}{2}\right).$$

To see why, one needs to make use of the following limit:

$$\lim_{x \to 0^+} \frac{\tan x}{x} = 1.$$

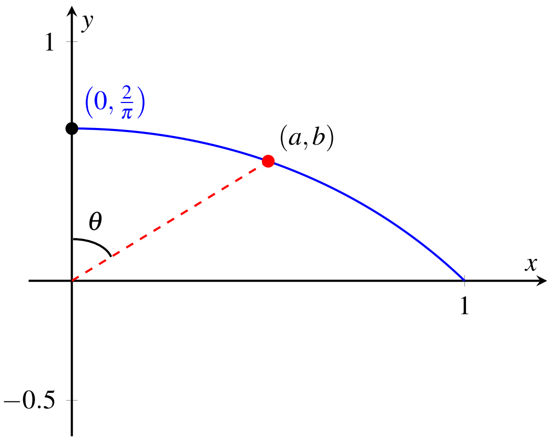


Figure 8: Graph of $y = x\cot\left(\frac{\pi x}{2}\right)$ for $0 < x \le 1$ with labeled point and angle θ

This means that the quadratrix meets the y-axis at $y = 2/\pi$. We will follow Hippias and include this point on the curve.

Next, we claim that we can square the circle starting from 0 and 1 and constructing new points using C1, C2, P1, P2 or P3, together with the intersections of constructible lines with the quadratrix. Note that $(2/\pi)\,i$ and i are constructible, and because $\mathscr{C}$ is a subfield of $\mathbb{C}$, it follows that π is constructible. By **(b)** of Theorem 9.1, it follows that $\sqrt{\pi}$ is constructible.

Now, let $r \in \mathbb{Q}^+$ be arbitrary. Consider a circle of radius r. Then,

$$\text{as } r, \sqrt{\pi} \text{ are constructible,} \quad \text{by field closure properties} \quad \text{we have } \pi r^2 \text{ also being constructible.}$$

As such, squaring the circle is permitted with the quadratrix!

We then discuss how the quadratrix can be helpful with angle trisection. In Figure 8, consider a point (a,b) on the quadratrix, which determines an angle θ. By some simple trigonometry,

$$\sin\theta = \frac{a}{\sqrt{a^2+b^2}} = \frac{a}{\sqrt{a^2+a^2\cot^2(a\pi/2)}} \quad \text{since} \quad (a,b) \text{ satisfies } y = x\cot\left(\frac{\pi x}{2}\right).$$

Using the Pythagorean identity $1+\cot^2\theta = 1/\sin^2\theta$, it follows that

$$\sin\theta = \sin\left(\frac{a\pi}{2}\right).$$

By injectivity, it follows that $\theta = a\pi/2$. For any angle $0 < \theta < \pi/2$, it follows that θ can be trisected starting from 0, 1, and θ and constructing new points using C1, C2, P1, P2 or P3, together with the intersections of constructible lines with the quadratic. By trisection, we mean that

$$\text{if } \theta \text{ is constructible} \quad \text{then} \quad \frac{\theta}{3} \text{ is also constructible.}$$

In general, thanks to the quadratrix, we can n-sect (not sure if this is an actual terminology) any angle θ, i.e. divide it into n equally sized angles θ/n.

The spiral of Archimedes also possesses the same property.

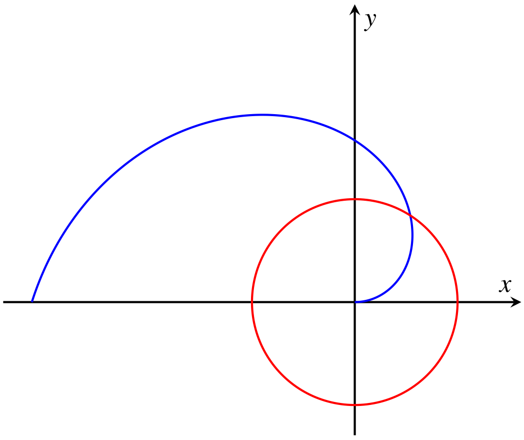


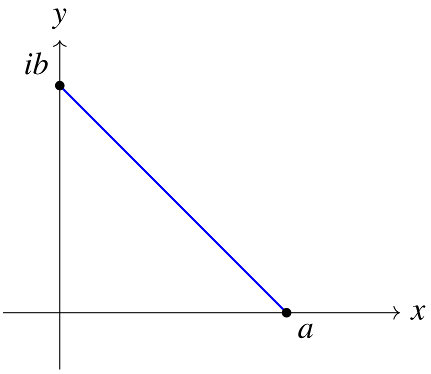
Figure 9: The Spiral of Archimedes $r = \theta$ and a unit circle

Definition 9.2 (field of Pythagorean numbers)**.** Let $\mathscr{P}$ denote the set of real numbers that can be obtained from 0, 1, and i by a sequence of straightedge-and-dividers constructions.

It is known that $\mathscr{P}$ is a subfield of $\mathbb{R}$. A more interesting property of $\mathscr{P}$ is that

$$a, b \in \mathscr{P} \quad \text{then} \quad \sqrt{a^2 + b^2} \in \mathscr{P}.$$

To see why, recall that the y-axis is constructible using $0, i$ and the straightedge (Example 9.2), so that given $b \in \mathscr{P}$, we can construct ib using our dividers. Combining this with $a \in \mathscr{P}$, we obtain the following diagram:



Now, we use the dividers to transfer the line segment from a and ib to the positive x-axis, starting from 0. Pythagoras' theorem implies that $\sqrt{a^2 + b^2} \in \mathscr{P}$ as claimed. In general, a subfield of $\mathbb{R}$ that contains $\sqrt{a^2 + b^2}$ whenever it contains a and b is called Pythagorean (Definition 9.2). This is in fact the smallest Pythagorean subfield of $\mathbb{R}$.

Analogous to Theorem 9.3, we have the following result about $\mathscr{P}$:

Theorem 9.4. Let $\alpha \in \mathbb{R}$ be algebraic over $\mathbb{Q}$, and let f be the minimal polynomial of α over $\mathbb{Q}$ with splitting field L. Then, the following are equivalent:

(a) $\alpha \in \mathscr{P}$

(b) All roots of f are real, and α is constructible

(c) All roots of f are real, and $[L:\mathbb{Q}]$ is a power of 2

In Definition 9.2, we defined the field $\mathscr{P} \subseteq \mathbb{R}$ and what it means for a subfield $F \subseteq \mathbb{R}$ to be Pythagorean. If $\alpha \in \mathbb{R}$, we have $\alpha \in \mathscr{P}$ if and only if there is a sequence of fields

$$\mathbb{Q} = F_0 \subseteq \ldots \subseteq F_n \subseteq \mathbb{R}$$

such that $\alpha \in F_n$ and for $i = 1, \ldots, n$, there are $a_i, b_i \in F_{i-1}$ such that $F_i = F_{i-1}\left(\sqrt{a_i^2 + b_i^2}\right)$.

It follows that $\mathscr{P}$ is the smallest Pythagorean subfield of $\mathbb{R}$.

9.2. *Regular Polygons and Roots of Unity*

It is of interest regarding which regular n-gons admit a straightedge and compass construction. Our main tool will be the cyclotomic extension $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ that was discussed in the previous chapter. Before we delve into the main result, we need to make use of the following terminology:

Definition 9.3 (Fermat prime). An odd prime p is

$$\text{a Fermat prime} \quad \text{if} \quad p = 2^{2^m} + 1 \text{ for some } m \in \mathbb{Z}_{\geq 0}.$$

Example 9.12 (Cox p. 274 Question 7). The Fermat primes are $3, 5, 17, 257, 65537$, which correspond to $m = 1, \ldots, 4$ respectively. It is conjectured that there are only 5 of them.

Although F_n commonly denotes the Fibonacci sequence, we will use F_n to denote the sequence of Fermat numbers (Fermat primes form a subset of this).

Example 9.13 (Cox p. 274 Question 8). Use

$$\log_{10}(F_{33}) \approx 2^{33}\log_{10}(2) \quad \text{to estimate the number of digits in the decimal expansion of } F_{33}.$$

Then, do the same for $F_{2478782}$.

Solution. We motivate our discussion with a known Fermat prime F_4. Recall that $F_4 = 65537$, so

$$\log_{10}(F_4) \approx 2^4 \log_{10}(2) = 4.8164 \approx 5.$$

So, the estimated number of digits in the decimal expansion of F_{33} is $2^{33}\log_{10}(2) \approx 2585827972.98 \approx 2585827973$ (obtained using Python); computing the number of digits in the decimal expansion of $F_{2478782}$ is much more difficult though. The interested reader can read up Pierpont primes, which are prime numbers of the form

$$2^u \cdot 3^v + 1 \quad \text{where } u, v \in \mathbb{Z}_{\geq 0}.$$

As part of the ongoing worldwide search for factors of Fermat numbers, some Pierpont primes have been announced as factors. Consider m, k, n such that

$$2^{2^m} + 1 \quad \text{is divisible by} \quad 3^k \cdot 2^n + 1.$$

In 2003, Cosgrave, Jobling, Woltman, and Gallot discovered that the tuple $(m,k,n) = (2478782,1,2478785)$ works. Also, the first edition of Cox's textbook was published in 2004. Coincidence? The second and current edition was published in 2010, but it was only in 2011 that Brown, Reynolds, Penne and Fougeron discovered a larger a larger m, with corresponding tuple $(m,k,n) = (2543548,2,2543551)$ □

Now, for the long-awaited moment — we are now ready to characterise constructible regular polygons using the Gauss-Wantzel theorem (Theorem 9.5)!

Theorem 9.5 (Gauss-Wantzel theorem)**.** Let $n > 2$ be an integer. Then, a regular n-gon admits a straightedge and compass construction if and only if

$$n = 2^s \prod_{i=1}^{r} p_i \quad \text{where } s \in \mathbb{Z}_{\geq 0} \text{ and the } p_i^\prime s \text{ are distinct Fermat primes.}$$

Proof. Constructing a regular n-gon is equivalent to constructing the n^{th} roots of unity $1, \zeta, \ldots, \zeta^{n-1}$ since they form the vertices of a unit regular n-gon. The roots of unity are constructible if and only if ζ is constructible since powers of constructible numbers are constructible. We note that

$$\zeta = \exp\left(\frac{2\pi i}{n}\right) = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$$

is constructible if and only if $\cos(2\pi/n)$ and $\sin(2\pi/n)$ are constructible. Moreover, by the Pythagorean identity $\cos^2\theta = 1 - \sin^2\theta$, the regular n-gon is constructible if and only if $\cos(2\pi/n)$ is constructible.

Let $\alpha = \cos(2\pi/n)$. Over the field $\mathbb{Q}(\alpha)$, note that ζ satisfies the equation $\zeta^2 - 2\alpha\zeta + 1 = 0$. Since $\mathbb{Q}(\alpha)$ consists of only real numbers, it follows that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)] = 2$. Then, by the tower theorem, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \phi(n)/2$, where $\phi(n)$ is Euler's Totient Function. This is because $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$.

It now suffices to prove the following:

- The regular n-gon is constructible if $\phi(n)$ is a power of 2
- If $\phi(n)$ is a power of 2, then the regular n-gon is constructible

The former is obvious by the repeated application of the tower theorem. As for the latter, suppose $\phi(n) = 2^m$. Then, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is an Abelian group of order a power of 2. The same is true for $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$. By the Fundamental Theorem of Abelian Groups that the Abelian Group G of order 2^m has a chain of subgroups

$$\{e\} = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_i \leq G_{i+1} \leq \ldots \leq G_{m-1} \leq G_m = G$$

with $[G_{i+1} : G_i] = 2$ for all i, applying this to $G = \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ and taking the fixed fields for the subgroups of G_i, we obtain the required sequence of quadratic extensions. To complete the proof, it suffices to show that a prime p with $p-1$ a power of 2 must be of the form $2^{2^m}+1$. We omit it. □

Example 9.14. Prove that a regular pentagon is constructible.

Solution. Consider the equation $z^5 = 1$. It is equivalent to $(z-1)\left(1+z+z^2+z^3+z^4\right) = 0$. Since $\zeta = e^{2\pi i/5}$ satisfies $1+z+z^2+z^3+z^4 = 0$, then $1+\zeta+\zeta^4+\zeta^2+\zeta^3 = 0$. We purposely wrote it this way so that the reader observes that

$$\zeta+\zeta^4 = 2\cos\left(\frac{2\pi}{5}\right) \quad \text{and} \quad \zeta^2+\zeta^3 = 2\cos\left(\frac{4\pi}{5}\right).$$

Hence, $1+2\cos(2\pi/5)-2\cos(4\pi/5) = 0$. By the double angle formula, it is easy to see that $\cos(2\pi/5)$ satisfies the equation $4x^2+2x-1 = 0$. Note that $4x^2+2x-1$ is irreducible over $\mathbb{Q}$ (show a contradiction when we attempt to factorise this polynomial into linear factors $\in \mathbb{Q}[x]$), so $[\mathbb{Q}(2\pi/5):\mathbb{Q}] = 2$, and the result follows. □

Around 1640, numbers of the form $2^{2^m}+1$ first appeared in Fermat's correspondence. He knew that they were prime for $0 \leq m \leq 4$ and conjectured that this was also true for $m \geq 5$, though he never found a rigorous proof. In 1729, Goldbach's first letter to the young Euler mentions Fermat's conjecture about $2^{2^m}+1$. Euler was sufficiently intrigued to start reading Fermat's letters. His first paper on number theory, published in 1732, shows that $F_5 = 2^{32}+1$ is divisible by 641, disproving Fermat's claim. Encouraged by this success, he went on to study other problems posed by Fermat over the course of the next 50 years. For example, he defined $\phi(n)$ in his attempt to understand Fermat's little theorem.

Because of Euler's negative result, there was little interest in Fermat primes until Gauss discovered their relation to the constructibility of regular polygons. The first entry in his famous mathematical diary, dated March 30, 1796, reads as follows:

> The principles upon which the division of the circle depend, and geometrical divisibility of the same into seventeen parts, etc.

The details of what Gauss proved about regular polygons appear in Section VII of his book titled '*Disquisitiones Arithmeticae*' (Latin for 'Arithmetical Investigations'). Gauss studied the equations satisfied by periods (special primitive elements of intermediate fields) of the extension $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p)$, where p is prime. Then, he applies his results to show that ζ_p is constructible when p is a Fermat prime. Though he asserts that the converse is true, the first published proof is due to Wantzel in 1837. Gauss describes which ζ_n are constructible when n is arbitrary (Theorem 9.5), though his proof is again incomplete.

Gauss knew that a straightedge-and-compass construction of a regular 17-gon was a big deal. Rather than give an explicit construction, he showed that

$$\cos\left(\frac{2\pi}{17}\right) = -\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}.$$

From here one can design a construction for the regular 17-gon, though it is inefficient. There is also the story of Professor Hermes of Lingen, who in the 19th century, worked 10 years on the construction of the regular 65537-gon.

Example 9.15 (Cox p. 273 Question 5). Let $n \geq 2$ and $\zeta_n = e^{2\pi i/n}$. Suppose that $n = 2^s p_1 \dots p_r$, where $p_1, \dots, p_r$ are distinct Fermat primes.

(a) Show that for $s \geq 1$, ζ_{2^s} is constructible.

(b) Let $a \geq 2$ and $b \geq 2$ be positive integers. Assume that ζ_a and ζ_b are constructible and $\gcd(a,b) = 1$. Show that ζ_{ab} is constructible.

We have omitted **(c)** of the exercise, which states that since $\zeta_{p_1}, \dots, \zeta_{p_r}, \zeta_{2^s}$ are constructible, then ζ_n is also constructible. Well, we briefly talk about this. Note that the Fermat primes are pairwise coprime, and none of them is even, so $p_1, \dots, p_r, 2^s$ are pairwise coprime. Since $n = 2^s p_1 \dots p_r$, by repeatedly using **(b)**, the result follows.

Solution.

(a) $[\mathbb{Q}(\zeta_{2^s}) : \mathbb{Q}] = 2^{s-1}$, which is a power of 2. The result follows.

(b) By Bézout's lemma, there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Thus, $x/b + y/a = 1/ab$. Since ζ_a and ζ_b are constructible, then ζ_a^x and ζ_b^y are constructible. Thus,

$$\zeta_{ab} = e^{2\pi i/ab} = e^{2\pi i(x/b + y/a)} = \zeta_a^x \zeta_b^y.$$

Since the product of two constructible numbers is constructible, the result follows. □

We conclude with some remarks about arc length. This was an important topic in the 17th and 18th centuries. For example, by inscribing a regular n-gon in the unit circle, one easily sees that constructing the n-gon by straightedge and compass is equivalent to dividing a circle into n equal arcs by straightedge and compass. Another example involves the lemniscate, which is the curve in the plane defined by the polar equation $r^2 = \cos 2\theta$ (Figure 10).

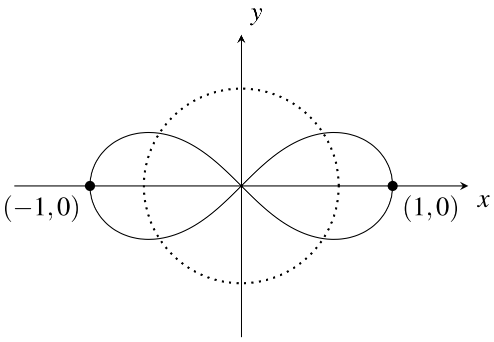


Figure 10: Lemniscate of Bernoulli

In 1716 Fagnano discovered a method for doubling and halving an arc of the lemniscate. In particular, he showed that the circle of radius $\sqrt{\sqrt{2} - 1}$ (see dashed circle in Figure 10) divides each quadrant of the lemniscate into arcs of equal length. Hence, the lemniscate can be divided into eight equal arcs by straightedge and compass.