2. BACKGROUND

§2.1. Sets and Functions

A **set** is a collection of 'things' called elements with $x \in \mathbf{S}$ indicating that x is an **element** (member) of the set S ($x \notin \mathbf{S}$ if it is not). A set can be described by listing its elements $\{a, b, ...\}$ or by specifying a defining property $\{x \in \mathbf{S} | \mathrm{P}x\}$ meaning the set of all $x \in$ S for which Px is true. We often omit the '$\in$ S' if it is understood and write $\{x | \mathrm{P}x\}$.

S is a **subset** of T if $x \in$ S implies that $x \in$ T and we denote this by $\mathbf{S} \subseteq \mathbf{T}$. Two sets are defined to be **equal** if each is a subset of the other. The set S is a **proper subset** of T ($\mathbf{S} \subset \mathbf{T}$) if S $\subseteq$ T and S $\neq$ T.

The **empty set** is $\varnothing$, the set with no elements. The **intersection** $\mathbf{S} \cap \mathbf{T} = \{x \mid x \in \mathrm{S} \text{ and } x \in \mathrm{T}\}$ and the **union** $\mathbf{S} \cup \mathbf{T} = \{x \mid x \in \mathrm{S} \text{ or } x \in \mathrm{T}\}$.

Important sets are:
$\mathbb{Z}$ = the set of integers,
$\mathbb{Q}$ = the set of rational numbers,
$\mathbb{R}$ = the set of real numbers and
$\mathbb{C}$ = the set of complex numbers.

A **map** (function) θ**:S→T** is a pair of sets
S (= **domain**) and
T (= **codomain**)
together with a rule that associates with every $x \in S$ a unique **image** $x^{\theta} \in T$. (It is more usual to write this as $\theta(x)$ but we shall reserve that notation for polynomials.)

The set of all the images of the elements of S is called the **image** of θ and is written **im** $\theta = \{x^{\theta} \mid x \in S\}$.
The map is **1-1** if $x^{\theta} = y^{\theta}$ implies that $x = y$ and **onto** if im $\theta = T$.

We say that θ **fixes** x, or x is a **fixed point** of θ, if $x^{\theta} = x$.
The **identity map** on a set S is the map $1:S \to S$ which fixes every element.

If $\alpha:X \to Y$ and $\beta:Y \to Z$ are maps we define their **product** $\alpha\beta:X \to Z$ by $x^{\alpha\beta} = (x^{\alpha})^{\beta}$, that is apply α first, then β.
(Note $\alpha\beta$ can be written as $\beta \circ \alpha$.).

§2.2. Complex Numbers

Complex numbers are of the form $z = x + iy$ where $x, y \in \mathbb{R}$**,** and **i** is an 'imaginary' number with $i^2 = -1$. Complex numbers are added and multiplied in the obvious way.

The cartesian form of a complex number is $x + iy$. If $z \neq 0$, the **polar form** of z is is $r(\cos\theta + i \sin\theta)$ where

$r \geq 0$ and $0 \leq \theta < 2\pi$. The **modulus** of z is $|\boldsymbol{z}| = r = \sqrt{x^2 + y^2}$ and the **argument** of z is $\arg \boldsymbol{z} = \theta$.

The **conjugate** of z is $\overline{\boldsymbol{z}} = x - iy$, so a complex number is real if and only if it is equal to its conjugate.

For $z \neq 0$, $z^{-1} = \dfrac{\overline{z}}{|z|^2}$ In particular, for complex numbers with modulus 1 (on the **unit circle**), $z^{-1} = \overline{z}$.

De Moivre's Theorem states that:
$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$ for all $n \in \mathbb{Z}$,
the first step towards justifying $e^{i\theta} = \cos\theta + i\sin\theta$.

The n'th roots of 1 are $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$ where $\varepsilon = e^{2\pi i/n}$, and for $n \geq 2$ their sum is 0 (the sum of the zeros of $z^n - 1$). In particular the cube roots of 1 are $1, \omega, \omega^2$ where $\omega = e^{2\pi i/3} = \dfrac{-1 + \sqrt{3}\, i}{2}$ and $1 + \omega + \omega^2 = 0$.

§2.3. Coordinate Geometry

The equation of the **line** passing through (x_1, y_1) and (x_2, y_2) is: $\boldsymbol{(y - y_1)(x_2 - x_1) = (x - x_1)(y_2 - y_1)}$ and the equation of the **circle** with centre (x_1, y_1) that passes through (x_2, y_2) is:

$$\boldsymbol{(x - x_1)^2 + (y - y_1)^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2.}$$

§2.4. Calculus

Real variable calculus studies real functions, that is, functions from $\mathbb{R}$ to $\mathbb{R}$. We refer to the **closed interval**

$$[a, b] = \{x \mid a \le x \le b\}$$

and the **open interval**

$$(a, b) = \{x \mid a < x < b\}.$$

If $f : \mathbb{R} \to \mathbb{R}$ we say that L is the **limit** of $f(x)$ as $x \to a$ if:

for all $\varepsilon > 0$ there exists $\delta > 0$ such that
$|x - a| < \delta$ implies that $|f(x) - L| < \varepsilon$.

We say that f is **continuous** at $x = a$ if the limit of $f(x)$, as $x \to a$, is $f(a)$ and that f is **differentiable**, at $x = a$, if the limit of $\dfrac{f(x) - f(a)}{x - a}$ as $x \to a$, exists. We call this limit $f'(x)$ and the function $\boldsymbol{f'}$ is called the **derivative** of f (with respect to x). We say that f is **continuous** or **differentiable** if it has that property at every point. Differentiability implies continuity. Polynomials have both properties.

Intermediate Value Theorem: If $f(x)$ is a continous function on the closed interval $[a, b]$ then if $f(a) < 0 < f(b)$ we must have $f(c) = 0$ for some c with $a < c < b$.
[Of course a similar result holds if $f(a) > 0 > f(b)$.]

Rolle's Theorem: If $f(x)$ is differentiable on the open interval (a, b) and continuous on the closed interval $[a, b]$ then if $f(a) = 0 = f(b)$ we must have

$$f'(c) = 0 \text{ for some } c \text{ with } a < c < b.$$

§2.5. Groups

Galois invented group theory for the purpose of answering the question "which polynomials have zeros that can be expressed in terms of its coefficients using the operations +, –, ×, ÷ and extraction of roots?" A **group** is an algebraic structure G with an associative operation (which we shall usually called multiplication) under which G is closed, and where there is an identity element, denoted by 1, with respect to which every element of G has an inverse. The **trivial group** is {1}. An **abelian group** is one which satisfies the commutative law.

A **subgroup** is a non-empty subset which is closed under multiplication and inverses, and a **proper subgroup** is one that is not G itself. **Notation: $\mathbf{H \leq G}$** and $H < G$, respectively.

Powers of elements are defined in the usual way and the **cyclic subgroup generated by g** is:

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$

A group G is **cyclic** if $G = \langle g \rangle$ for some $g \in G$, called a **generator**. Cyclic groups are abelian. The **order of a group** G is its size $|G|$ and the **order of an element** g is the order of the subgroup $\langle g \rangle$. The **index** of a subgroup

H is **|G:H|**, the number of left (or right) cosets and for finite groups it is |G|/|H|.

If $H \leq G$ a **left coset** is a set of the form $xH = \{xh \mid h \in H\}$ and a **right coset** is one of the form $Hx = \{hx \mid h \in H\}$. All cosets have the same number of elements, this being |H|. The group G decomposes into a disjoint union of cosets of either type from which it follows that the order of a subgroup (and hence the order of an element) of a finite group, G, divides |G|.

If $Hx = xH$ for all $x \in G$ we say that H is a **normal subgroup** of G and in such cases we can form a group, called the **quotient group** G/H, from these cosets with the coset H as its identity. A **simple group** is one with no proper non-trivial normal subgroup. Subgroups of index 2 are normal.

The **cyclic group of order *n*** is denoted by $\mathbf{C}_n$. The **dihedral group** $\mathbf{D}_{2n}$ (of order $2n$) can be expressed in terms of generators and relations as:

$$\langle A, B \mid A^n = B^2 = 1, BA = A^{-1}B \rangle$$

with D_4 more usually written as $\mathbf{V}_4$. D_{2n} is non-abelian if and only if $n \geq 3$. Groups of prime order are cyclic and groups of order $2p$ must be cyclic or dihedral.

A group **homomorphism** is a map $f:G \to H$, from one group to another which preserves products and an **isomorphism** is a 1-1 and onto homomorphism. If an isomorphism exists between G and H we say that G, H are **isomorphic** and we write $\mathbf{G \cong H}$.

The **kernel** of a homomorphism f is:
ker f = $\{g \in G \mid g^f = 1\}$ and the **image** of f is
im f = $\{g^f \mid g \in G\}$.

The First Isomorphism Theorem states that ker f is a normal subgroup of G, im f is a subgroup of H and G/ker f ≅ im f. Consequences are:
Second Isomorphism Theorem: if H, K ≤ G, with K being normal, then HK/K ≅ H/(H∩K);
Third Isomorphism Theorem: if H ≤ K ≤ G with both H, K being normal in G, then (G/H)/(G/K) ≅ K/H.

Two elements *h*, *k* of a group G are **conjugate** in **G** if $h = g^{-1}hg$ for some $g \in G$. The relation of being conjugate is an equivalence relation, breaking G into equivalence classes. The number of conjugates of *g* is $|G:C_G(g)|$, where $C_G(g)$ is the **centralizer** of *g* in G, the group of elements that commute with g. Similar properties hold for subgroups of G. Two subgroups, H, K of a group G are **conjugate** in **G** if

$H = g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$ for some $g \in G$.

The number of conjugates of H is $|G:N_G(H)|$, where $N_G(H)$ is the **normalizer** of H, the set $\{g \in G \mid g^{-1}Hg = H\}$.

A **commutator** is an element of the form:

$$[x, y] = x^{-1}y^{-1}xy.$$

The **derived subgroup** of a group G is **G′**, which is the subgroup generated by all its commutators. A useful characterisation of G′ is that it's the smallest normal

subgroup for which the quotient is abelian. The **derived series** is $G \geq G' \geq G'' \geq ...$ and if this series reaches 1 we say that G is **soluble**.

If p^n divides |G|, where p is prime, then G has at least one subgroup of order p^n. In particular if p^n is the largest power of p which divides |G| then such a subgroup is called a **Sylow *p*-subgroup**. These are all conjugate in G and their number is congruent to 1 modulo p and divides |G|.

The direct sum of abelian groups $G_1, ..., G_k$ under addition is $G_1 \oplus ... \oplus G_k = \{(x_1, ..., x_k) \mid \text{each } x_i \in G_i\}$ with point-wise addition. Every finite abelian group is a direct sum of cyclic groups of prime power order.

§2.6. Permutations

For Galois, all groups were groups of permutations on the zeros of polynomials. A **permutation** on a set X is a 1-1 map from X to itself. The most efficient notation is **cycle notation**:

$$(x_1\ x_2\ ...\ x_r)(y_1\ ...\ y_s)\ ....$$

where each symbol maps to the one on its right, except for the last in each cycle which maps to the first. Cycles of length 1 are omitted, except for the identity permutation which is denoted by I. The **symmetric group S_n** is the set of all $n!$ permutations on $\{1, 2, ..., n\}$ under multiplication of functions.

An ***n*-cycle** is a permutation of the form $(x_1 \ldots x_n)$ and a **transposition** is a 2-cycle. Every permutation is a product of cycles and each n-cycle is a product of $n - 1$ transpositions so every permutation is a product of transpositions. An **even (odd**) permutation is one which is a product of an even (odd) number of transpositions and no permutation can be both, so cycles of odd length are even. Permutations satisfy the rules:

$$\text{even} \times \text{even} = \text{even},$$
$$\text{even} \times \text{odd} = \text{odd},$$
$$\text{odd} \times \text{even} = \text{odd},$$
$$\text{odd} \times \text{odd} = \text{even}.$$

The **alternating group $\mathbf{A}_n$** is the subgroup of $\mathbf{S}_n$ consisting of the even permutations. If $n > 1$, $\mathbf{A}_n$ has index 2 in $\mathbf{S}_n$ and so is normal. For $n \geq 5$, $\mathbf{A}_n$ is simple and so $\mathbf{A}_n$ and $\mathbf{S}_n$ are not soluble for these n.

§2.7. Fields and Rings

The modern view of Galois Theory is that it is the study of fields using group theory as a tool, though the concept of a field came much later than Galois. A **field** is an algebraic system which consists of a set F, together with two binary operations + and × such that F is an abelian group under addition, $F^{\#}$, the non-zero elements, are an abelian group under multiplication and such that the distributive law holds.

Familiar examples are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. There are also finite fields, of which the simplest are the fields, $\mathbb{Z}_p$, of integers modulo a prime. A **subfield** of a field is a subset which is a field under the same operations, so $\mathbb{Q}$ and $\mathbb{R}$ are examples of subfields of $\mathbb{C}$.

A **ring** is a more general structure, again with two operations of addition and multiplication, where the distributive law holds. But whereas the ring must be an abelian group under addition the only requirements for multiplication are closure and the associative law. The ring of integers, $\mathbb{Z}$, is a commutative ring and, if $n \geq 2$, the ring $M_n(F)$ of all $n \times n$ matrices over F is an example of a non-commutative ring.

An **integral domain** is a commutative ring with a 1, in which the cancellation law holds – that is:

If $xy = 0$ then $x = 0$ or $y = 0$.

A **field** is an integral domain in which every non-zero element has a multiplicative inverse.

§2.8. Vector Spaces

A **vector space** over a field F is a set V together with two operations: addition and multiplication by a **scalar** (an element of F). Under addition a vector space must be an abelian group. Additional axioms involving scalar multiplication are:

- $\lambda v \in V$,
- $(\lambda + \mu)v = \lambda v + \mu v$,
- $\lambda(u + v) = \lambda u + \lambda v$,

- $(\lambda\mu)v = \lambda(\mu v)$ and
- $1v = v$.

Note that I'm not following the usual convention of denoting vectors in bold type to distinguish them from scalars. The reason is that in Galois Theory both vectors and scalars are numbers.

A **subspace** is a subset that is a vector space under the same operations. **Notation: $\mathbf{U \leq V}$**.

We tend to think of vectors as having components, such as (x, y, z) and as such are quite distinct from scalars. However the axioms don't insist on this. By comparing the axioms for fields and those for vector spaces we can see that fields can be viewed as vector spaces over any subfield, in which case the elements of the subfield will be both a vector and a scalar.

A **linear combination** of vectors $v_1, v_2, \ldots v_n$ is an expression of the form

$$\lambda_1 v_1 + \ldots \lambda_n v_n$$

where the λ_i's are scalars and the v_i's are vectors. It is **non-trivial** if at least one $\lambda_i \neq 0$. A set of vectors X **spans** a vector space if every vector in the space is a linear combination of the vectors in X. It is **linearly independent** if no non-trivial linear combination is zero (otherwise it is **linearly dependent**). A **basis** for V is a linearly independent subset which spans V. A vector space is **finite-dimensional** if it has a finite spanning set. Every finite-dimensional vector space V has a basis and

all bases have the same number of vectors, called the **dimension** of V (**dim** V). Any subset smaller than dim V can't span V and any set bigger than dim V must be linearly dependent.

Any field extension [K:F] is a vector space where the elements of F are the vectors and the elements of K are the scalars (as well as also being some of the vectors.) The dimension of the field extension is simply the dimension of F as a vector space over K. It is written as **|K:F|**.

A **linear transformation** f:U→V, from one vector space over F to another, is a map which preserves addition and scalar multiplication.

The **kernel** of f is (**ker f**) = $\{v \in V | v^f = 0\}$ and the **image** (**im f**) = $\{v^f \mid v \in V\}$ are subspaces of U, V respectively. The **rank** of a linear transformation is the dimension of the image and the **nullity** is the dimension and the kernel and **rank + nullity = dim (domain)**.

§2.9. Polynomials

In the middle ages, solving polynomial equations was the main problem of algebra and solving the quintic was what inspired Galois. A **polynomia**l over a field F is an expression of the form $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ where the **coefficients** $a_0, ... , a_n \in$ F and where x is an 'indeterminate'. Coefficients of higher powers are

assumed to be zero. A polynomial is usually written in the form a(x) and if a quantity α (in F, or a field containing F) is **substituted** for x the value obtained is written **a(α)**. Polynomials are regarded as equal if corresponding coefficients are equal. The set of all polynomials over F is denoted by **F[x]**. Polynomials can be added and multiplied in the usual way and under these operations F[x] is an integral domain, though not a field. In fact the ring of polynomials behave very much like the ring of integers, with greatest common divisors and primes.

The polynomial $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ has **degree** n if $a_n \neq 0$, in which case a_n is called the **leading coefficient**. (The degree of the zero polynomial is undefined.). A polynomial is **monic** if its leading coefficient is 1. A polynomial of degree 0 is a non-zero **constant polynomial**. There are special names for polynomials of low degree: **Linear polynomials** have degree 1, **quadratics** have degree 2, and the list extends to **cubics**, **quartics** and **quintics**. When polynomials multiply their degrees add, so degree is like a crude sort of logarithm.

The so-called **Division Algorithm** for integers, that justifies quotients and remainders, also applies to polynomials. It states that every polynomial a(x) $\in$ F[x] can be divided by a non-zero polynomial b(x), giving a **quotient** q(x) and a **remainder** r(x), both in F[x], where the remainder is either zero or has lower degree than b(x).

A simple consequence is the **Remainder Theorem** which states that the remainder on dividing $a(x)$ by $x - \alpha$ is $a(\alpha)$.

A **zero** of a polynomial $a(x)$ is a number α for which $a(\alpha) = 0$. Any non-real zeros of a real polynomial come in conjugate pairs. Real polynomials of odd degree have at least one real zero (by continuity). More generally, the **Fundamental Theorem of Algebra** states that every non-constant polynomial over $\mathbb{C}$ has a zero in $\mathbb{C}$. This can be proved using the techniques of complex variables, but in a later chapter we'll give a proof that is algebraic.

If the remainder on dividing $a(x)$ by $b(x)$ is zero we say that $b(x)$ **divides** $a(x)$. Divisibility properties of polynomials are very similar to those of integers. In particular we define a non-constant polynomial to be **prime** if it cannot be written as a product of polynomials of lower degree. (The constant polynomials are excluded for technical reasons, similar to those that exclude the number 1 from being called a prime.)

Prime polynomials over $\mathbb{Q}$ have distinct zeros. [If $(x - \alpha)^2$ divides $p(x)$ then $x - \alpha$ divides both $p(x)$ and $p'(x)$ and so $p(x)$ and $p'(x)$ are not coprime.]

We define the **greatest common divisor** of two non-zero polynomials $a(x)$, $b(x)$ to be the monic polynomial of highest degree which divides them both. We denote it by **GCD**$[a(x), b(x)]$ and if the GCD is 1 we say that the polynomials are **coprime**.

As with integers there's a method for computing the GCD called **the Euclidean Algorithm**. This involves dividing one polynomial by another and then repeatedly dividing the most recent remainder by the one before. Eventually we get a zero remainder and the last non-zero remainder, made monic, is the GCD. A consequence of this algorithm is the fact that the GCD of a(x) and b(x) can be expressed in the form:

$$a(x)h(x) + b(x)k(x)$$

for some polynomials h(x), k(x) over the same field.

The quadratic formula, $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ for the quadratic $ax^2 + bx + c$ expresses the zeros in terms of its coefficients using the operations +, –, ×, ÷ and extraction of roots (radicals). As we'll see, there are similar (though more complicated) formulae for cubic and quartic polynomials, but not for quintics and beyond.

In the following table we set out the parallel between integers and polynomials.

INTEGERS	**POLYNOMIALS**
Division Algorithm: If a, $b \in \mathbb{Z}$ with $b \neq 0$ there exist q, $r \in \mathbb{Z}$ such that $a = bq + r$ and $\lvert r \rvert < \lvert b \rvert$.	**Division Algorithm:** If a(x), b(x) $\in$ F[x] with b(x) $\neq$ 0 there exist q(x), r(x) $\in$ F[x] such that a(x) = b(x)q(x) + r(x) and r(x) = 0 or deg r(x) < deg b(x).

We call r the **remainder** on dividing a by b.	We call $r(x)$ the **remainder** on dividing $a(x)$ by $b(x)$.
b **divides** a if $a = bq$ for some $q \in \mathbb{Z}$. **Notation:** $b \mid a$.	$b(x)$ **divides** $a(x)$ if $a(x) = b(x)q(x)$ for some $q(x) \in F[x]$. **Notation:** $b(x) \mid a(x)$.
D(a) = {divisors of a}.	**D($a(x)$)** = {divisors of $a(x)$}.
$D(a) \cap D(b)$ is the set of **common divisors** of a, and b.	$D(a(x)) \cap D(b(x))$ is the set of **common divisors** of $a(x)$ and $b(x)$.
A **greatest common divisor** of a, b is a common divisor of a, b with greatest absolute value.	A **greatest common divisor** of $a(x)$, $b(x)$ is a common divisor of $a(x)$, $b(x)$ with greatest degree.
u is a **unit** if $u^{-1} \in \mathbb{Z}$. The units are ± 1.	$u(x)$ is a **unit** if $u(x)^{-1} \in F[x]$. The units are the non-zero constant polynomials.
a, b are **associates** if $a = bu$ for some unit u, or equivalently if they divide each other or equivalently if $a = \pm b$.	$a(x)$, $b(x)$ are **associates** if $a(x) = b(x)u(x)$ for some unit $u(x)$, or equivalently if they divide each other or equivalently if $a(x) = kb(x)$ for some non-zero k.
Any two greatest common divisors of a, b are associates of one another.	Any two greatest common divisors of $a(x)$, $b(x)$ are associates of one another.

THE greatest common divisor is the +ve one. **Notation: GCD(a, b)**.	THE greatest common divisor is the monic one. **Notation: GCD(a(x), b(x))**.
If d = GCD(a, b) then $d = ah + bk$ for some $h, k \in \mathbb{Z}$.	If d(x) = GCD(a(x), b(x)) then d(x) = a(x)h(x) + b(x)k(x) for some h(x), k(x) $\in$ F[x].
p is **prime** if $\|p\| > 1$ and whenever $p = ab$ either a or b is a unit.	p(x) is **prime** if deg p(x) > 0 and whenever p(x) = a(x)b(x) either a(x) or b(x) is a unit.
n is **composite** if it is not zero, not a unit and not prime.	f(x) is **composite** if it is not zero, not a unit and not prime.
If a prime integer divides a product it must divide one of the factors.	If a prime polynomial divides a product it must divide one of the factors.
Every composite integer can be factorised uniquely into primes. (Uniqueness means that the factors can be paired so that corresponding prime factors are associates.)	Every composite polynomial can be factorised uniquely into primes. (Uniqueness means that the factors can be paired so that corresponding prime factors are associates.)

I won't provide proofs here for any of the above results, though the proofs for polynomials are easily adapted from the proofs of the corresponding results for

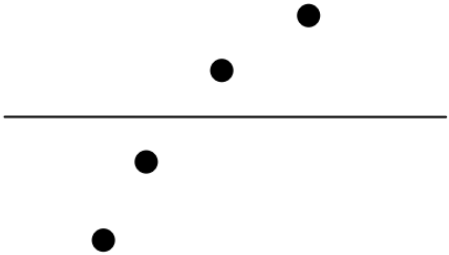
integers. The most satisfactory thing to do, if we'd had the time, would be to develop the theory of a certain type of ring called a **Euclidean Ring**. These rings include the ring of integers as well as the ring of polynomials over a field. The above definitions and properties would then just become particular instances of the general theory. Euclidean Rings are discussed in my notes on *Ring Theory*.

§2.10. Numbers of Real Zeros

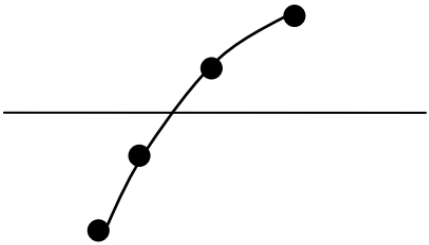
In order to find insoluble polynomials we need to be able to determine the number of real zeros of a real polynomial. This may seem easy – just draw the graph and count how many times the curve cuts the x-axis.

This is all very well, but if we want an absolutely rigorous proof that a polynomial is insoluble we need to consider two important difficulties. Drawing a graph means plotting a finite number of points and guessing what happens in between. Even if we obtain exact values of the ordinates of these points we are making assumptions about the intermediate values. We can always decide to plot many more points, but at the end of the day we will have only finitely many points.

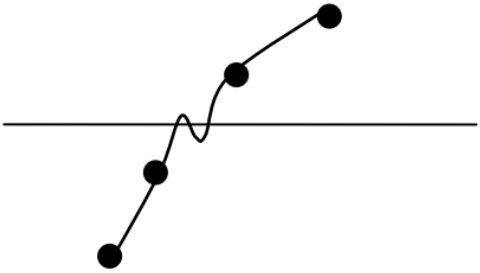
Suppose we have the following points plotted.



Since polynomials are continuous we know, by the Intermediate Value Theorem, that there is at least one real zero in this interval. Here it would be very reasonable to suppose that there is just one real zero.

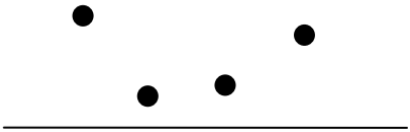


But it could be that there are three (or even more) real zeros, very close together.

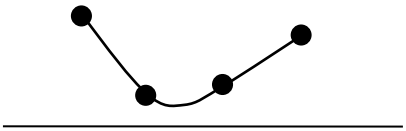


In order to be absolutely sure we would need to find the number of real zeros of the derivative of this polynomial in this interval. That in turn would lead to the same problems and we would have to investigate higher and higher derivatives until we reach a quadratic.

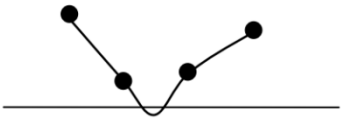
A second problem is the following. Suppose we have plotted (exactly) the following four points.



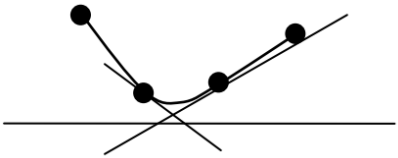
It would be reasonable to guess that there are no real zeros in this interval.



But there could be two (or even more).



To settle the question we would have to look at tangents. If indeed there were no zeros we would be able to find points close enough so that the tangents intersect above the *x*-axis. (Of course we'd have to ensure that the curves did not intersect these tangents further.)



To carry out this careful analysis on a quintic would be quite a deal of work, and as we are interested here in the algebra, and not calculus, we will be content to simply plot the graph and hope that we've used enough points to see what's going on.

EXERCISES FOR CHAPTER 2

Exercise 1: If S = {1, 2, 4, 5} and T = {1, 3, 4, 6} write down $S \cap T$.

Exercise 2: How many proper non-empty subsets are there of {1, 3, 4}.

Exercise 3: Is the map θ: $\{x \in \mathbb{R} \mid x > 0\} \to \mathbb{Z}$ defined by $x^{\theta} = \text{INT}(\log x)$ a 1-1 function? Is it onto? Here INT means the integer part.

Exercise 4: If f : $\mathbb{R} \to \mathbb{R}$ and g: $\mathbb{R} \to \mathbb{R}$ are defined by: $x^{f} = x^2$ and $x^{g} = 2^x$ find 3^{fg} and 3^{gf}.

Exercise 5: Write down the fixed points of f:$\mathbb{R}\to\mathbb{R}$ defined by $x^{f} = x^2 - 4x + 6$.

Exercise 6: Find the modulus, conjugate and inverse of the complex number $i - 2$.

Exercise 7: Simplify $\omega + \omega^2$.

Exercise 8: Write down all five fifth roots of 1 in terms of $\varepsilon = e^{2\pi i/5}$.

Exercise 9: If $\varepsilon = e^{2\pi i/7}$ find the conjugate of ε^3 as a power of ε.

Exercise 10: Which real number(s) can be expressed as a sum of two cube roots of 1?

Exercise 11: If A = (1, –3) and B = (3, 5) find the equations of the line through A, B and the circle with centre A which passes through B.

Exercise 12: Is $F = \{a + bi \mid a, b \in \mathbb{Q}\}$ a field?

Exercise 13: Is $F = \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$ a field?

Exercise 14: Is {(2, 1), (4, 2)} a basis for $\mathbb{R}^2$?

Exercise 15: Are the vectors (1, 1), (2, 5), (3, 17) linearly independent?

Exercise 16: If $f:\mathbb{R}^7 \to \mathbb{R}^3$ is a linear transformation whose image is $\{(x, y, x + y) \mid x, y, z \in \mathbb{R}\}$ find the dimension of ker f.

Exercise 17: Find the zeros, over $\mathbb{Q}$, of the polynomial

$$x^2 + 5x + 6.$$

Exercise 18: "The polynomial $x^5 + 17x^4 - 33x + 2$ has exactly 2 real zeros and 3 non-real zeros." Why must this statement be false?

Exercise 19: "The polynomial $x^4 - 3x^7 + 32$ has four non-real zeros and no real ones." Why must this claim be false?

Exercise 20: If a real polynomial $f(x)$ has a non-real zero α, find a real quadratic factor.

Exercise 21: Which real polynomials over $\mathbb{R}$ are prime over $\mathbb{R}$?

Exercise 22: Find GCD$(x^3 + 1, x^2 + 2x + 1)$ and express it in the form

$$(x^3 + 1)h(x) + (x^2 + 2x + 1)k(x)$$

for suitable rational polynomials $h(x)$, $k(x)$.

Exercise 23: If G is the group

$$\langle A, B \mid A^4 = B^2 = 1, BA = A^{-1}B \rangle$$

what is $|G|$?

Exercise 24: What is the order of the complex number i under multiplication?

Exercise 25: Write down a proper non-trivial subgroup of the cyclic group generated, under multiplication, by the complex number i.

Exercise 26: "The group G has order 100 and has 5 subgroups of order 6". Why must this statement be false?

Exercise 27: If $|G| = 17$, find all the subgroups of G.

Exercise 28: For which of the following values of n: 3, 4, 5, 6, 7, 8 is there a cyclic group of order n. For which of these values of n is there no other group of order n?

Exercise 29: The set $G = \{1, 3, 7, 9, 11, 13, 17, 19\}$ is a group under multiplication modulo 20 and $H = \{1, 11\}$ is a normal subgroup. Find the cosets of H in G. Which of the groups $\mathbf{C}_4$ and $\mathbf{C}_2 \times \mathbf{C}_2$ is isomorphic to G/H?

Exercise 30: Let $f: \mathbb{R}^{\#} \to \mathbb{R}$ be defined by $x^f = \log(x^2)$, where $\mathbb{R}$ is the group of all real numbers under addition and $\mathbb{R}^{\#}$ is the group of all non-zero real numbers under multiplication. Show that f is a homomorphism and find ker f and im f. Hence find a quotient group of $\mathbb{R}^{\#}$ which is isomorphic to $\mathbb{R}$.

Exercise 31: Which abelian groups are soluble?

Exercise 32: If $|G'| = 4$, why must G be soluble?

Exercise 33: Why is D_{60} a soluble group?

Exercise 34: "The group G has order 80 and only 4 proper non-trivial subgroups." Why must this statement be false?

Exercise 35: What is are the orders of the Sylow subgroups of a group of order 1125?

Exercise 36: If a = (12345) and b = (12), find $(ab)^{-2}b(ab)^2$.

Exercise 37: Is $(1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9) \in \mathbf{A}_9$?

Exercise 38: $\mathbf{A}_4$ has a normal abelian subgroup $\mathbf{V}_4$ of order 4. Why does it follow that $\mathbf{S}_4$ is soluble?

Exercise 39: For which values of n is $\mathbf{S}_n$ soluble?

Exercise 40: If a = (1452376) and b = (27) find the order of the group they generate.

SOLUTIONS FOR CHAPTER 2

Exercise 1: $S \cap T = \{1, 4\}$.

Exercise 2: 6.

Exercise 3: It is onto but not 1-1.

Exercise 4: $3^{fg} = 2^9$ and $3^{gf} = 2^6$.

Exercise 5: These are the values of x for which $x^2 - 4x + 6 = x$, namely 2, 3.

Exercise 6: The modulus is $\sqrt{5}$, the conjugate is $-i - 2$ and the inverse is $-\frac{2 + i}{5}$.

Exercise 7: -1.

Exercise 8: $1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4$.

Exercise 9: ε^4.

Exercise 10: 2 and -1.

Exercise 11: The equation of AB is:
$\frac{y + 3}{x - 1} = \frac{5 + 3}{3 - 1} = \frac{8}{2} = 4$, which simplifies to $y = 4x - 7$.

The equation of the circle is:
$(x - 1)^2 + (y + 3)^2 = (3 - 1)^2 + (5 + 3)^2 = 68$.
This simplifies to $x^2 + y^2 - 2x + 6y - 58 = 0$.

Exercise 12: YES. Since $\frac{1}{a + b\mathrm{i}} = \frac{a - b\mathrm{i}}{a^2 + b^2} \in \mathrm{F}$ if $a + b\mathrm{i} \neq 0$, it satisfies the property that every non-zero element has a multiplicative inverse. The other field properties are obvious.

Exercise 13: NO because $(\sqrt[3]{2})^2 \notin \mathrm{F}$.

Exercise 14: NO. They are not linearly independent.

Exercise 15: NO. The space of vectors (x, y) has dimension 2 and so any more than 2 vectors will be automatically linearly dependent.

Exercise 16: The rank of f is the dimension of the image. It is clearly 2. The nullity is therefore $7 - 2 = 5$. This is the dimension of ker f.

Exercise 17: $-2, -3$.

Exercise 18: Non-real zeros of a real polynomial come in conjugate pairs and hence there must always be an even number of them.

Exercise 19: It has degree 7 (the first term is not always the leading term!). Since 7 is odd the polynomial must have a real zero.

Exercise 20: The conjugate $\bar{\alpha}$ must also be a zero and hence $(x - \alpha)(x - \bar{\alpha})$ must be a real quadratic factor. This can be written as $x^2 - 2\text{Re}(\alpha) + |\alpha|^2$.

Exercise 21: Linear polynomials, of the form $ax + b$ (where $a \neq 0$) and quadratics of the form $ax^2 + bx + c$ where $b^2 < 4ac$. (Note that this automatically includes the condition that $a \neq 0$.)

Exercise 22:

$$\begin{array}{r l}
 & x - 2 \\
x^2 + 2x + 1 \,) & \overline{x^3 + 1} \\
 & \underline{x^3 + 2x^2 + x} \\
 & -2x^2 - x + 1 \\
 & \underline{-2x^2 - 4x - 2} \\
 & 3x + 3
\end{array}$$

Clearly dividing $x^2 + 2x + 1$ by $x + 1$ we get a remainder of zero, so the last non-zero remainder, made monic, is $x + 1$.

From the above, $3x + 3 = (x^3 + 1) - (x^2 + 2x + 1)(x - 2)$
Hence we can take $h(x) = \frac{1}{3}$ and $k(x) = \frac{1}{3}(x - 2)$.

Exercise 23: 8.

Exercise 24: 4.

Exercise 25: $\{1, -1\}$.

Exercise 26: 6 does not divide 100, so this contradicts Lagrange's Theorem.

Exercise 27: Just 1 and G because 17 is prime.

Exercise 28: All of them. The integers 3, 5 and 7.

Exercise 29: $H = \{1, 11\}$, $3H = \{3, 13\}$, $7H = \{7, 17\}$, $9H = \{9, 19\}$. $(3H)^2 = 9H \neq H$ so 3H has order 4. This means that $G/H \cong \mathbf{C}_4$.

Exercise 30: $(xy)^f = \log((xy)^2)$
$= \log(x^2y^2)$
$= \log(x^2) + \log(y^2)$
$= x^f + y^f$.
$\ker f = \{x \in \mathbb{R}^\# \mid \log(x^2) = 0\}$
$= \{x \in \mathbb{R}^\# \mid x^2 = 1\}$
$= \{1, -1\}$.
im f = $\mathbb{R}$**.**
Hence $\mathbb{R}^\#/\{1, -1\} \cong \mathbb{R}$.

Exercise 31: All of them.

Exercise 32: Groups of order 4 are abelian, so $G'' = 1$.

Exercise 33: $\mathbf{D}_{60} = \langle A, B \mid A^{30} = A^2 = 1, BA = A^{-1}B \rangle$.
Let $H = \langle A \rangle$. Then $\mathbf{D}_{60}/H$ has order 2 and so $\mathbf{D}_{60}' \leq H$. But H is abelian, so $\mathbf{D}_{60}'' = 1$.

Exercise 34: By Sylow's Theorem there exists a subgroup of order p^n when ever the prime power p^n divides the group order. Hence G has subgroups of orders 2, 4, 8, 16 and 5.

Exercise 35: $1125 = 3^2.5^3$. So the Sylow 3-subgroups have order 9 and the Sylow 5-subgroups have order 125.

Exercise 36: $ab = (2\ 3\ 4\ 5)$ and so $(ab)^2 = (2\ 4)(3\ 5)$.
Hence $(ab)^{-2}b(ab)^2 = [(2\ 4)(3\ 5)]^{-1}(1\ 2)[(2\ 4)(3\ 5)]$
$= (1\ 4)$.

Exercise 37: YES. It is an even permutation.

Exercise 38: $|\mathbf{S}_4/\mathbf{A}_4| = 2$ so $\mathbf{S}_4' \leq \mathbf{A}_4$.
$|\mathbf{A}_4/\mathbf{V}_4| = 3$ so $\mathbf{A}_4/\mathbf{V}_4$ is cyclic and hence abelian, so $\mathbf{S}_4'' \leq \mathbf{A}_4' \leq \mathbf{V}_4$.
Since groups of order 4 are abelian, $\mathbf{S}_4''' \leq \mathbf{V}_4' = 1$.

Exercise 39: $n = 1, 2, 3$ and 4.

Exercise 40: They generate $\mathbf{S}_7$, which has order $7! = 5040$.