Lecture 27
POLYNOMIALS

"Polynomials" transliterates as "many numbers". This refers to the coefficients a_j's of the x^j's in $\sum_{j=0}^{n} a_j x^j$. Before we discuss such things therefore, it is imperitive that we come to a more intimate understanding of number systems.

Standard Notations for Number Systems.

Nonnegative integers: $\mathbb{N}$ (**N**atural numbers, or cardinal numbers)
$\mathbb{N} := \{0, 1, 2, \dots\}$.
$\mathbb{N}$ can be constructed purely set theoretically. The *Fundamental Theorem of Arithmetic* states that the natural numbers greater than 1 can be written uniquely as the product $\Pi_{i=1}^{s} p_i^{\alpha_i}$ for *prime* numbers p_i and positive natural numbers s and α_i. The way this works is not yet fully understood and largely depends on the *Riemann Hypothesis* which has not yet been proven (Bombieri, 2000).

Nonpositive integers: $\mathbb{N}^-$
$\mathbb{N}^- := \{\dots, -2, -1, 0\}$

Integers: $\mathbb{Z}$ (German: **Z**ahlen=numbers)
$\mathbb{Z} := \mathbb{N} \cup \mathbb{N}^-$

Positive integers: $\mathbb{Z}^+ = \mathbb{P}$
$\mathbb{Z}^+ = \mathbb{P} := \mathbb{N} \backslash \{0\}$.

Negative integers: $\mathbb{Z}^-$
$\mathbb{Z}^- := \mathbb{N}^- \backslash \{0\}$

Rational numbers: $\mathbb{Q}$ (**Q**uotients)
$\mathbb{Q} := \left\{ \frac{p}{q} : p \in \mathbb{Z} \ \& \ q \in \mathbb{Z} \backslash \{0\} \right\}$

Positive rational numbers: $\mathbb{Q}^+$
$\mathbb{Q}^+ := \left\{ \frac{p}{q} : p, q \in \mathbb{Z}^+ \right\}$

Negative rational numbers: $\mathbb{Q}^-$
$\mathbb{Q}^- := \{ \frac{p}{q} : p \in \mathbb{Z}^- \ \& \ q \in \mathbb{Z}^+ \}$

Real numbers: $\mathbb{R}$
$\mathbb{R}$ can be constructed from $\mathbb{Q}$. It is easier but less rigorous to simply say there is a 1-1 correspondence between $\mathbb{R}$ and the real number line. $\mathbb{R}$ is up to isomorphism the only complete ordered field.

Positive real numbers: $\mathbb{R}^+$
$\mathbb{R}^+ := \{r \in \mathbb{R} : r > 0\}$
(where "$r > 0$" means that r occurs to the right of 0 on the real number line).

Negative real numbers: $\mathbb{R}^-$
$\mathbb{R}^- := \{r \in \mathbb{R} : r < 0\}$
(where "$r < 0$" means that r occurs to the left of 0 on the real number line).

All the above number systems are one dimensional.

Complex numbers: $\mathbb{C}$ - two dimensional numbers
$\mathbb{C} := \{a + ib, c + id : a, b, c, d \in \mathbb{R},\ i$ is an *arbitrary symbol* such that $(a + ib) + (c + id) = (a + c) + i(b + d)$ & $(a + ib)(c + id) = (ac - bd) + i(bc + ad)\}$
Letting $a = c = 0,\ \&\ b = d = 1$ we see from this definition that $i^2 = -1$.

The notations e (for $\sum_{n=0}^{\infty} \frac{1}{n!}$) and i (for $\sqrt{-1}$) were invented by Leonard Euler. These numbers have been very influential in mathematics.

Another notation (William Rowan Hamilton's) for complex numbers is as ordered pairs $(a, b)(= a + ib)$ where $a, b \in \mathbb{R}$ but this is rarely used thesedays.

Quaternion numbers: $\mathbb{H}$ (for **H**amilton who invented them) - four dimensional numbers

Octonion numbers: $\mathbb{O}$ - eight dimensional numbers

$\mathbb{C}$, $\mathbb{H}$, & $\mathbb{O}$ are all based on $\mathbb{R}$ and the units 1 and i, j, k, l, m, n, o which are such that $i^2 = j^2 = k^2 = l^2 = m^2 = n^2 = o^2 = -1$. $\mathbb{H}$ and $\mathbb{O}$ are defined similarly to $\mathbb{C}$ together with other conditions on i, j, k, l, m, n, o.

Theorem. $\mathbb{P} \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}$.

Occasionally in the literature, we see $\mathbb{N}$ confused with $\mathbb{P}$. We also see the notation $\mathbb{P}$ used for a **p**rojective set. In these notes however, we will use these symbols as they are defined above.

In this notation I am using $\mathbb{BLACKBOARD\ BOLD}$ font, and this is also how we handwrite them, but we often see them typed in **BOLD** font, i.e.:

$$\mathbf{P}, \mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{H}, \mathbf{O}.$$

An older and less frequently used notation is (in MEDIUM ROMAN font):

J for integers
R for rationals
R* for reals

C for complex numbers

We can generalise complex numbers to n-dimensional *hypercomplex* numbers $\sum_{j=1}^{n} i_j a_j$ where $n \in \mathbb{Z}^+,\ a_j \in \mathbb{R}$, $i_1 = 1$ and $i_2^2 = \cdots = i_n^2 = -1$, as well as several other conditions on the i_j's. However, we actually don't need number systems with dimensions other than 1, 2, 4 or 8. In particular, if $\mathbb{S}$ is a finite dimensional division algebra over $\mathbb{R}$, then the dimension of $\mathbb{S}$ as a vector space over $\mathbb{R}$ is equal to 1, 2, 4 or 8. This was first suspected as early as the early 1800's. There are now several proofs of this and of several equivalent statements in the literature. But it was first proved in the 1950's by Milnor who built upon the work of Bott (Milnor, 1958) and independently by Kervaire (Kervaire, 1958).

Sometimes however, we use the notations $\mathbb{X}^*$ for the *extended* number system of $\mathbb{X}$ where $\mathbb{X}$ is one of the number systems above.
$\mathbb{X}^* := \mathbb{X} \cup \{\infty\}$ or $\mathbb{X} \cup \{-\infty\}$ or $\mathbb{X} \cup \{-\infty, \infty\}$.

The notation $\mathbb{R}^*$ is also sometimes used to represent the *hyperreal* number system, which is the same as $\mathbb{R}$ but with the added axiom of calculus that *infinitessimals* δx exist. **Applied** mathematicians are famous (or infamous, depending on your perspective) for using the idea of infinitessimals as if they were elements of $\mathbb{R}$ and they have had great success in so doing. Pure mathematicians will tell you that they are not elements of $\mathbb{R}$. However, if we use this notion as an **axiom** and in so doing **replace** $\mathbb{R}$ by $\mathbb{R}^* := \mathbb{R} \cup \{\delta x\}$ it is possible to construct a **pure** mathematical calculus system without the use of limits. Calculus questions in $\mathbb{R}$ will still have solutions in $\mathbb{R}$ but with the help of $\mathbb{R}^*$ instead of limits. Applied mathematicians will just tell you "I told you so". But the main difference between pure and applied mathematicians is that applied mathematicians are comfortable with "fudge factors" and pure mathematicians are not. Pure mathematicians will tell you there is no way they will accept the notion of infinitessimals until they have a good way of **understanding why it works**. Applied mathematicians will tell you they will accept an idea **because it works**, whether they understand it or not! The theory of hyperreals has helped to blur the distinction between pure and applied mathematics. In any case, due to Kurt Gödel's undecideablity theorem which states that any logical mathematical system will contain unproveable statements, this may be a vacuous point. But such theorems do not diminish the level of precision present throughout mathematics coupled with the self imposed burden of proof, which is as it always has been, superior in this regard compared with other academic disciplines.

All New South Wales high school students will be familiar with all the abovementioned number systems except $\mathbb{C}$, $\mathbb{H}$, & $\mathbb{O}$. Complex numbers are used in many applications in physics and engineering, and quaternion and octonion numbers are used in high level physics such as quantum mechanical angular momentum and some aspects of the theory of superstrings.

$\mathbb{Z}$ is an *integral domain* (has closure of addition & multiplication, commutivity and associativity of addition and multiplication, distributivity of multiplication over addition, additive and multiplicative identities, additive inverses and a cancellation law) and $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are *fields* (are integral domains and also have multiplicative inverses). Hence

these are the most useful of all number systems, and so most of mathematics only uses $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, & $\mathbb{C}$ and nothing else. Nevertheless, many other integral domains and fields are used in pure mathematical research. Note that $\mathbb{H}$ and $\mathbb{O}$ are **not** fields.

There is a 1-1 correspondence between $\mathbb{Z}$ and $\mathbb{Q}$ which is especially interesting since one of these is only an integral domain whereas the other is a field. Anything in 1-1 correspondence with $\mathbb{Z}$ is called *countable*.

There is no 1-1 correspondence between $\mathbb{Z}$ and $\mathbb{R}$. This is often articulated by saying that $\mathbb{R}$ is *uncountable*. There is also no 1-1 correspondence between $\mathbb{R}$ and $\mathbb{C}$.

Theorem. $\mathbb{R}$ *is not countable,* $\mathbb{C}$ *is not ordered,* $\mathbb{H}$ *is not commutative,* $\mathbb{O}$ *is not associative* (Baez, 2001).

If we redefine $\mathbb{Q}$ by saying it is the set of solutions for x to all equations of the form $a_1 x + a_0 = 0$ for integers a_0, a_1 with $a_1 \neq 0$ then we can see that we can generalise $\mathbb{Q}$ to $\mathbb{A}$, the set of all *algebraic numbers* which are real solutions to polynomial equations $\sum_{j=0}^{n} a_j x^j = 0$ for integers $a_0, \ldots, a_n$ where $a_n \neq 0$. For example, $\sqrt{2}$, which is irrational, is nevertheless algebraic. $\mathbb{A}$ is countable. So $\mathbb{T} := \mathbb{R} \backslash \mathbb{A}$, the set of all *trancendental numbers*, is uncountable. e and π are transcendental. We will see in Lecture 29 that all polynomial equations with coefficients in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ have solutions in $\mathbb{C}$, so sometimes we see a different definition of the set of algebraic numbers than the one given above, allowing it to have complex elements. This is still countable. The trancendental compliment of this set with respect to $\mathbb{C}$ is likewise uncountable. But this definition isn't common because a complex number is of the form $a + ib$ for real a, b so a trancendental complex number can be defined such that inclusively a or $b \in \mathbb{T}$. Similarly an algebraic complex number can be defined such that a and $b \in \mathbb{A}$.

There is also a hypothesis called Georg Cantor's Continuum Hypothesis which says that for any superset $\mathbb{X}$ of $\mathbb{Z}$ which is also a subset of $\mathbb{R}$, i.e., for any set $\mathbb{X}$ such that $\mathbb{Z} \subset \mathbb{X} \subset \mathbb{R}$ there is either a 1-1 correspondence between $\mathbb{Z}$ and $\mathbb{X}$ or there is a 1-1 correspondence between $\mathbb{X}$ and $\mathbb{R}$. This was proved to be undecideable within the confines of Cantorian set theory in 1963 by Paul Cohen (i.e., the truth or otherwise or this mathematical hypothesis not only trancends the mathematics from which it emerged, but is also independent of it). Nevertheless, logical systems can be constructed within which it can be proved **and** other (more exotic) logical systems can be constructed within which it can be disproved!

So I guess we should not frown upon applied matematicians with too much scorn and derision for their obsessive preponderance on fudge factors.

Examples of factorising over $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$.

Example 1. Factorise $x^4 - 4$ over $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$.

$$\begin{aligned} x^4 - 4 &= (x^2 - 2)(x^2 + 2) \ \leftarrow \text{ completely factorised over } \mathbb{Z} \\ &= (x - \sqrt{2})(x + \sqrt{2})(x^2 + 2) \ \leftarrow \text{ completely factorised over } \mathbb{R} \\ &= (x - \sqrt{2})(x + \sqrt{2})(x^2 - (i\sqrt{2})^2) \\ &= (x - \sqrt{2})(x + \sqrt{2})(x - i\sqrt{2})(x + i\sqrt{2}). \ \leftarrow \text{ completely factorised over } \mathbb{C} \quad \square \end{aligned}$$

Example 2. Factorise $x^2 + x + 1$ over $\mathbb{C}$

$$\begin{aligned} x^2 + x + 1 &= x^2 + x + \tfrac{1}{4} + \tfrac{3}{4} \\ &= (x + \tfrac{1}{2})^2 + \tfrac{3}{4} \\ &= (x + \tfrac{1}{2})^2 - \left(\tfrac{i\sqrt{3}}{2}\right)^2 \\ &= \left(x + \tfrac{1}{2} - \tfrac{i\sqrt{3}}{2}\right)\left(x + \tfrac{1}{2} + \tfrac{i\sqrt{3}}{2}\right). \quad \square \end{aligned}$$

Example 3. Factorise $2x^2 + 3x - 1$ over the complex field.

$$\begin{aligned} 2x^2 + 3x - 1 &= 2\big(x^2 + \tfrac{3}{2}x - \tfrac{1}{2}\big) \\ &= 2\big(x^2 + \tfrac{3}{2}x + \tfrac{9}{16} - \tfrac{1}{2} - \tfrac{9}{16}\big) \\ &= 2\big(\big(x + \tfrac{3}{4}\big)^2 - \tfrac{17}{16}\big) \\ &= 2\Big(x + \tfrac{3-\sqrt{17}}{4}\Big)\Big(x + \tfrac{3+\sqrt{17}}{4}\Big). \quad \square \end{aligned}$$

Lecture 28

More Examples.

Example 1. Factorise $P(x) = x^3 - 4x^2 + 14x - 20$ completely over the complex field.

Test for factors of 20, i.e., $\pm 1, \pm 2, \pm 4 \pm 5, \pm 10, \pm 20$.

$P(1) \neq 0,\ P(2) = 0$ & $\therefore (x-2)$ is a factor.

$$\begin{aligned} P(x) &= (x-2)(x^2 - 2x + 10) \\ &= (x-2)(x^2 - 2x + 1 + 9) \\ &= (x-2)((x-3)^2 + 3^2) \\ &= (x-2)((x-3)^2 - (3i)^2) \\ &= (x-2)(x-3-3i)(x-1+3i) \quad \square \end{aligned}$$

Example 2. Solve $P(x) = x^3 - 3x^2 + 4x - 2 = 0$ over $\mathbb{C}$.

Test $(\pm 1, \pm 2) \Rightarrow p(1) = 0$

$$\begin{aligned} \& \therefore (x-1)(x^2 - 2x + 2) &= 0 \\ \therefore (x-1)(x^2 - 2x + 1 + 1) &= 0 \\ \therefore (x-1)((x^2-1)^2 - i^2) &= 0 \\ \therefore (x-1)(x-1-i)(x-1+i) &= 0 \\ \& \therefore x = 1, 1 \pm i \quad \square \end{aligned}$$

Example 3. Solve $P(x) = x^3 - 1 = 0$ over $\mathbb{C}$.

$$\begin{aligned} P(1) &= 0 \\ \therefore (x-1)(x^2 + x + 1) &= 0 \\ \therefore (x-1)(x^2 + x + \tfrac{1}{4} + \tfrac{3}{4} &= 0 \\ \therefore (x-1)\Big(\big(x+\tfrac{1}{2}\big)^2 - \big(\tfrac{\sqrt{3}i}{2}\big)^2\Big) &= 0 \\ \therefore (x-1)\big(x + \tfrac{1}{2} - \tfrac{\sqrt{3}i}{2}\big)\big(x + \tfrac{1}{2} + \tfrac{\sqrt{3}i}{2}\big) &= 0 \\ \& \therefore x = 1, -\tfrac{1}{2} \pm \tfrac{\sqrt{3}i}{2} \quad \square \end{aligned}$$

Lecture 29

The Fundamantal Theorem of Algebra. *Every polynomial $P(x)$ with complex coefficients is such that $P(\alpha) = 0$ for some complex α.*

There are numerous proofs of this widely available in many texts, for example some such proofs can be found in the Schaum Outline *Complex Variables* (Spiegel, 1981).*

From this we can deduce the

Corollary. *Any polynomial of degree $n, (n > 0)$ has exactly n zeros in the field of complex numbers and hence exactly n linear factors.*

Proof. $P(x)$ is any polynomial $(n > 0)$. By the fundamental theorem of algebra $P(x)$ has at least one zero, $\alpha_1 \Rightarrow (x - \alpha_1)$ is a factor of $P(x) \Rightarrow P(x) = (x - \alpha_1)Q(x)$ for some polynomial $Q(x)$ over $\mathbb{C}$ but by the fundamental theorem of algebra, $Q(x)$ has at least one zero, $\alpha_2 \Rightarrow (x-\alpha_2)$ is a factor of $Q(x) \Rightarrow P(x) = (x-\alpha_1)(x-\alpha_2)R(x)$ for some polynomial $R(x)$ over $\mathbb{C}$ and this process continues until $P(x) = k(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ for some constant k (i.e., the coefficient of x^n) which shows that $P(x)$ has n linear factors, and n zeros. $\square$

It follows from this that $P(x)$ cannot have more than n roots and $P(x)$ is completely reducible to linear factors.

Note that if a complex number α is a zero of a polynomial $P(x) = \sum_{j=0}^{n} a_j x^j$ with real coefficients, then $P(\overline{\alpha}) = \sum_{j=0}^{n} a_j \overline{\alpha}^j = \overline{\sum_{j=0}^{n} a_j \alpha^j} = \overline{P(\alpha)} = \overline{0} = 0$ and so the complex conjugate $\overline{\alpha}$ of α is also a zero of $P(x)$. Hence $(x-\alpha)(x-\overline{\alpha}) = (x^2 - 2\Re(\alpha)x + |\alpha|^2) \Rightarrow P(x)$ can be broken down (i.e., is reducible) to a combination of real linear and quadratic factors.

*I highly recommend the *Schaum Outlines* for undergraduates who feel that the mountains of cellulose in university libraries are intimidatingly quagmirish. It is quagmirish, but if they proceed to postgraduate studies they would then more likely consult the American Mathematical Society's *Mathematical Reviews* and will then feel less intimidated, but until then, nothing brings stuff together quite like the *Schaum Outlines*. They have outlines in many other subjects too which are equally as impressive.

Example. Show that $x-(1+i)$ is a factor of $P(x)=x^3+2x^2-6x+8$. Hence factorise $P(x)$ over $\mathbb{R}$ and over $\mathbb{C}$.

$$\begin{aligned}P(1+i) &= (1+i)^3+2(1+i)^2-6(1+i)+8\\ &= 1+3i-3-i+2(1+2i-1)-6-6i+8\\ &= -2+2i+2+4i-2-6-6i+8\\ &= 0\end{aligned}$$

Hence $x-(1+i)$ is a factor of $P(x)$.

$1+i$ and $\overline{1+i}=1-i$ are zeros of $P(x)$ since $x-(1+i)$ is a factor of $P(x)$ and $P(x)$ has real coefficients & $\therefore (x-(1+i))(x-(1-i))=x^2-2x+2$ is a factor of $P(x)$. The constant term in $P(x)$ is 8 and the constant term in this factor is 2 and the leading coefficient of $P(x)$ is 1 & $\therefore (x+4)$ is a factor of $P(x)$ (since $4\times 2=8$). So

$$\begin{aligned}P(x) &= (x+4)(x^2-2x+2) \text{ over } \mathbb{R}\\ &= (x+4)(x-1-i)(x-1+i) \text{ over } \mathbb{C}. \quad \square\end{aligned}$$

Lecture 30

Zeros of multiplicity.

Example 1. If $P(x) = (x-4)^5(x-3)$, 4 is a zero of $P(x)$ of multiplicity 5.
Zeros are 4, 4, 4, 4, 4, 3.

Theorem. *If a is a zero of $P(x)$ of multiplicity m, then $P'(x)$ will have a as a zero of multiplicity $m-1$.*

Proof. $P(x) = (x-a)^m Q(x)$ for some polynomial $Q(x)$

$$\begin{aligned} P'(x) &= m(x-a)^{m-1}Q(x) + (x-a)^m Q'(x) \\ &= (x-a)^{m-1}(mQ(x) + (x-a)Q'(x)) \\ &= (x-a)^{m-1}R(x) \text{ for some polynomial } R(x) \quad \square \end{aligned}$$

Example 2. If $P(x) = x^4 + 2x^3 - 12x^2 + 14x - 5$ has a 3-fold zero, find the zeros of $P(x)$.

$$\begin{aligned} P'(x) &= 4x^3 + 6x^2 - 24x + 14 && - 2 \text{ fold} \\ P''(x) &= 12x^2 + 12x - 24 && - 1 \text{ fold} \\ &= 12(x^2 + x - 2) \\ &= 12(x+2)(x-1) \\ P(1) &= 0 \end{aligned}$$

$\therefore$ 1 is the 3 fold zero of $P(x)$. $\therefore$ the other zero is -5. $\therefore P(x) = (x-1)^3(x+5)$. $\therefore$ the zeros are 1, 1, 1, 5. $\square$